NUREG/CR–6265
BNL–NUREG–52431

Multidisciplinary Framework for Human Reliability Analysis with an Application to Errors of Commission and Dependencies

Prepared by
M. T. Barriere, BNL, J. Wreathall, JW&Co., S. E. Cooper, SAIC,
D. C. Bley, PLG, W. J. Luckas, Jr., BNL, A. Ramey-Smith, NRC

Brookhaven National Laboratory
John Wreathall and Company
Science Applications International Corporation
PLG, Incorporated

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

NUREG/CR-6265
BNL-NUREG-52431

Multidisciplinary Framework for Human Reliability Analysis with an Application to Errors of Commission and Dependencies

Manuscript Completed: July 1995
Date Published: August 1995

Prepared by
M. T. Barriere, BNL, J. Wreathall, JW&Co., S. E. Cooper, SAIC,
D. C. Bley, PLG, W. J. Luckas, BNL, A. Ramey-Smith, NRC

Contractor
Brookhaven National Laboratory
Upton, NY 11973

Subcontractors
John Wreathall and Company
Dublin, OH 43017

Science Applications International Corporation
Reston, VA 22090

PLG, Incorporated,
Newport Beach, CA 92660

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

Since the early 1970s, human reliability analysis (HRA) has been considered to be an integral part of probabilistic risk assessments (PRAs). Nuclear power plant (NPP) events, from Three Mile Island through the mid-1980s, showed the importance of human performance to NPP risk. Recent events demonstrate that human performance continues to be a dominant source of risk. In light of these observations, the current limitations of existing HRA approaches become apparent when the role of humans is examined explicitly in the context of real NPP events. The development of new or improved HRA methodologies to more realistically represent human performance is recognized by the Nuclear Regulatory Commission (NRC) as a necessary means to increase the utility of PRAs. To accomplish this objective, an Improved HRA Project, sponsored by the NRC's Office of Nuclear Regulatory Research (RES), was initiated in late February, 1992, at Brookhaven National Laboratory (BNL) to develop an improved method for HRA that more realistically assesses the human contribution to plant risk and can be fully integrated with PRA. This report describes the research efforts including the development of a multidisciplinary HRA framework, the characterization and representation of errors of commission, and an approach for addressing human dependencies. The implications of the research and necessary requirements for further development also are discussed.

CONTENTS

CONTENTS (Cont'd)

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Background

Since the early 1970s, human reliability analysis (HRA) has been considered as an integral part of probabilistic risk assessments (PRAs). Although various approaches and methods have been used since the first HRA was performed two decades ago as part of the Reactor Safety Study (WASH-1400) sponsored by the Nuclear Regulatory Commission (NRC), the technology still is not fully developed. Better integration of human reliability into the PRA process has long been a recognized NRC concern.

Existing HRA methods have been criticized for not realistically representing the roles humans play in preventing, initiating and mitigating nuclear power plant (NPP) accidents. Generally, these criticisms are that HRA methods cannot adequately address or accommodate underlying human contributions to severe accidents.

Severe accidents and other recent events, e.g., Three Mile Island Unit 2 (1979), Chernobyl Unit 4 (1986), Prairie Island Unit 2 (1992), Salem Unit 1 (1994), and Wolf Creek (1994), as well as recent NRC studies, such as NUREG-1275 and NUREG-1449, indicate that human performance is a dominant source of risk for all modes of plant operation (i.e., at power and shutdown). These accidents involved human errors of commission (EOCs), i.e., human actions initiating the event or complicating its recovery, including terminating engineered safety features and initiating inappropriate systems or procedures.

These significant contributions to plant risk are not reflected by the human errors typically modeled in current PRAs, e.g., NRC-mandated Individual Plant Examinations (IPEs), which primarily include human errors of omission (EOOs), such as omitting a proceduralized step or failing to initiate a safety-related function. This limited modeling is due largely to the constraints imposed by HRA methods that are not specifically designed to adequately account for EOCs, for the associated dependent actions that span the temporal phases of an accident, or for new plant conditions created by human-system interactions. Furthermore, current HRA methods do not support the integration of these human performance characteristics into PRAs.

The problem for HRA/PRA analysts is a lack of guidance for identifying and representing EOCs, their dependencies, and the interrelationship between plant conditions and human-system interactions in a PRA. Fragmented efforts at development have generated separate, non-integrable models reflecting a lack of communication among the relevant disciplines, i.e., human factors, behavioral science, and plant operations and systems engineering. In addition, current HRA methods are not based on actual operating experience and fail to consider explicitly the context in which people perform.

Consequently, PRAs have lacked credibility in their representation of the full contribution of human performance to NPP safety, particularly since human error has proved to be the dominant factor in NPP incidents. Without the explicit, realistic representation of human-performance characteristics identified in real events, PRA can only partially reflect the causes of risk.

To address these concerns, the NRC recognized 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 based on analyzing risk-significant human performance from NPP 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 this report)
(3) Development Phase (FY 95/96, ongoing)
(4) Implementation Phase (FY 96, planned)

The Assessment Phase consisted of an initial evaluation of potentially risk-significant human performance based on operating experience discussed in NRC Incident Investigation Team (IIT)/Augmented Inspection Team (AIT) reports, AEOD Human Performance Studies, and other NRC studies (e.g., NUREG-1275 and NUREG-1449), and also based on interviews with NRC staff and licensed operators. These evaluations noted the significant influence that plant conditions and performance shaping factors (PSFs) can have on EOCs that degrade plant safety and depend on prior human actions. NUREG/CR-6093, "An Analysis of Operational Experience During LP&S and a Plan for Addressing Human Reliability Assessment Issues," documented the Assessment Phase.

This report describes the Analysis and Characterization Phase encompassing the following activities:

(1) developing a multidisciplinary HRA framework for analyzing operating experience and improving the integration of HRAs with PRAs;

(2) characterizing EOCs and human dependencies and providing general guidance for identifying and representing them in PRAs; and

(3) conducting an independent peer review of the accomplishments to incorporate suggestions for modifications, and to make recommendations for further developments.

We also discuss the research implications, requirements for development, and regulatory applications for the project's Development and Implementation phases.

Overview of Results

The Analysis and Characterization Phase contributed considerably to improving PRA by expanding the boundary of what HRA can model and contributing a depth of realism to PRAs that was impractical previously. To do this, a multidisciplinary HRA framework was developed to provide a structured approach for analyzing operating experience and understanding NPP safety, human error, and the underlying factors that affect them. To be able to identify the necessary requirements for HRA, the framework had to be multidisciplinary because the factors affecting human reliability and plant safety are based on many sciences.

Multidisciplinary HRA Framework

By integrating the diverse disciplines of plant operations, systems engineering, human factors, and behavioral sciences, as well as HRA and PRA, into a framework, we identified important risk-significant contexts and their influence on human actions. The framework clarified perceived conflicts between these disciplines by bringing together their different languages and promoting mutual understanding. Elements of the framework depict the interrelationships between unsafe human actions, their associated error mechanisms, and the influences of plant conditions and PSFs on those mechanisms. In addition, for integration with PRAs, the framework also identifies how unsafe human actions should be incorporated into human failure events and discusses their relationship to plant states modeled in the PRA.

Retrospective analyses of operational events showed that the framework can reveal underlying factors that influence humans to perform unsafe actions and also can provide a basis for systematically evaluating the significance and characteristics of EOCs and their mechanisms. Thus, important aspects of EOCs and dependency mechanisms can be considered in developing an improved HRA method, and the requirements are clarified for more realistically including them in PRA models. The framework's common language and structure for relating the different dimensions of human-system interactions proved that evaluations of EOCs and dependencies can be tractable and tenable.

Considering the importance of these issues in NPP safety, this change is an important advance; without such a framework, systematically identifying the factors surrounding these errors would be extremely difficult. This systematic structuring of the different dimensions influencing human-system interactions brings a degree of clarity and completeness to the modeling of human errors; its lack previously limited the ability to incorporate human errors in PRAs in a way that could satisfy both the engineering aspects and the behavioral sciences.

Errors of Commission and Human Dependencies

One major goal is to appropriately model and quantify EOCs and human dependencies, which are of concern because they are involved in significant operational events. Based on our research, we found that out of the range of all possible EOCs, improvements in modeling focusing on those leading to dependent effects of other human errors are most vital to assuring the completeness and accuracy of PRAs. Consequently, these EOCs require new analysis through improvements in HRAs. The following EOC and dependency results are described in this report:

- characterization of the potential causes and consequences of EOCs and dependencies, and
- development of guidance for HRA and PRA analysts in representing potentially risk-significant EOCs and dependencies in PRA models.

Identifying the important characteristics of EOCs and dependencies required breaking from the familiar perspective on human-reliability influences and the underlying assumptions of PRA models. By analyzing events in the context of the multidisciplinary framework, plant conditions, PSFs, and instrumentation were found to be very influential factors for identifying, representing, and quantifying the occurrence and consequences of EOCs and dependencies.

An EOC is represented in the multidisciplinary HRA framework as a PRA term describing the potential manifestations of a human failure event on the hardware portion of the PRA model. Only those actions

that degrade plant safety functions, safety systems, or other risk-relevant equipment should be modeled as EOC human failure events in the PRA. This representation gives boundaries to the many actions that potentially could be labeled "errors of commission."

A taxonomy of dependence causal mechanisms, identified through the multidisciplinary framework and the analysis of operating events, supported an understanding of the underlying causes of dependent unsafe actions. This taxonomy consisted of common processes, common PSFs, and plant conditions. Common processes encompass deficient management decisions, work organization and planning, and other programmatic functions within the plant or utility, which simultaneously lead to poor or erroneous performance in most departments, and between work teams within departments. Common PSFs relate to the identified effects that procedures, controls and displays, or training, for example, had on significantly increasing the likelihood of error for all human actions relying on them. Plant conditions significantly contributed to the context within which activities were performed (e.g., shutdown conditions) and, therefore, significantly influenced the potential for multiple dependent failures.

Analyses of Events

Analyses of events played a large role in this research. They influenced the development of the multidisciplinary HRA framework, as well as the characterization of and guidance for modeling EOCs and dependencies. As the project evolved, different kinds of data and different perspectives from their analysis gave us significant insights that were supported by the continued development of a database designated the Human-System Event Classification System (HSECS). The database will provide critical support to future tasks, and will furnish descriptive information for the quantification process.

From the analyses and database classification of events, we found that the richest sources of human-reliability information were in the detailed descriptions of events given in NRC AEOD Human Performance Studies, followed next by NRC IIT and regional AIT reports, and full-text licensee event reports.

Independent Peer Review

After the Analysis and Characterization Phase was completed, our progress was independently reviewed by NRC representatives from the Offices of Regulatory Research (RES), Nuclear Reactor Regulation (NRR), Analysis and Evaluation of Operational Data (AEOD), and Nuclear Materials Safety and Safeguards (NMSS), as well as by consultants from universities, national laboratories, and independent organizations who were invited to review our progress because of their involvement in related work.

In general, the reviewers confirmed the project's results and potential applications. They agreed that the approach was valid, of extensive utility to NRC, and would enhance the PRA process. They recommended valuable modifications and additions for future efforts, giving suggestions for other regulatory applications. These recommendations involved using the framework and supporting database for assisting the NRC in its on-going efforts to gather and analyze data by providing analysts with tools for understanding operating events from a human reliability perspective, and potentially improving future event reporting (e.g., LERs, AITs/IITs, and AEOD Human Performance Studies) and diagnostic evaluations.

Overview of Research Implications and Future Plans

The broad implication of this research is that PRAs can more realistically reflect NPP risk by considering the elements of the multidisciplinary HRA framework, especially those related to EOCs and human dependencies. The fundamental concepts for improving the HRA process are in place and have allowed retrospective analyses of real operating-event histories, which have identified the context in which severe events can occur. More specifically, analyses of operational events have shown that (1) EOCs occur frequently and include human-induced initiators, (2) mechanisms for human dependencies based on plant conditions, common PSFs, and common organizational processes play an important role in the development of an event, and (3) human performance is significantly influenced by the combination of PSFs and plant conditions.

However, using the framework for prospective analysis remains to be specified, i.e., defining the context so that important EOCs and dependencies can be identified and predicted. To accomplish this and to provide an improved approach for HRA that incorporates operating experience, the implications of the research and the results of the independent peer review were integrated into further requirements that must be resolved in the project's remaining Development and Implementation phases.

The following requirements were identified for development:

(1) relating an expanded description of human-system interactions to PRA modeling,

(2) finalizing the multidisciplinary framework to more explicitly interpret error mechanisms and plant conditions,

(3) extending the HSECS database to better support the classification and description of real-world events involving human-system interactions, and

(4) developing an approach for using expert judgment that incorporates real-world operating experience and can support modeling and quantification.

Each of these requirements is discussed in this report. These efforts should lead to an improved HRA method that provides guidance on identifying and incorporating human failure events into PRA logic models and on obtaining information to quantify the probabilities of such events, and also shows how these probabilities can be estimated and incorporated into the overall PRA quantification process.

After this development is completed, the results will be incorporated into guidelines as part of the Implementation Phase and will be demonstrated on a suitable PRA. The guidelines will enable non-project team members (e.g., HRA and PRA analysts) to use the developed methodology.

By providing guidance and realistic human-performance data on which to base and develop PRA models, these efforts are consistent with the NRC's directions for current and future uses of PRA set out in the PRA Implementation Plan proposed by SECY-94-219, the PRA Working Group's NUREG-1489 (1994), and the November 2, 1993, memorandum from NRC Office Directors to the NRC Executive Director for Operations.

ACKNOWLEDGMENTS

The authors wish to give special thanks to the NRC/RES Project Management, especially Catherine M. Thompson for her significant contribution to the project's independent peer review process and program plan development. In addition, the encouragement and guidance of Joseph A. Murphy and Mark A. Cunningham have been very constructive and are appreciated.

We are grateful for the valuable input provided by the independent NRC project reviewers, James P. Bongarra, Jr. of NRR/HHFB, Joel Kramer and Carl E. Johnson, Jr. of RES/HFB, Dale M. Rasmuson of AEOD/TPAB, and Patricia A. Rathbun of NMSS/IMNS, as well as the non-NRC reviewers including George Apostolakis of the University of California at Los Angeles, John A. Forester of Sandia National Laboratories, David I. Gertman and Dana L. Kelly of the Idaho National Engineering Laboratory, Gareth W. Parry of Halliburton NUS Corporation, and James T. Reason of the University of Manchester, United Kingdom.

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, Robert E. Hall, John H. Taylor and William S. Brown. Special thanks are given to Pamela L. Ciufo and Kathleen M. Nasta for their outstanding assistance in preparing the manuscript and Avril D. Woodhead for her technical editorial review.

ACRONYMS

AEOD	NRC Office of Analysis and Evaluation of Operational Data
AIT	Augmented Inspection Team
ATWS	Anticipated Transient Without Scram
BNL	Brookhaven National Laboratory
BWR	Boiling Water Reactor
EOC	Error of Commission
EOO	Error of Omission
EP	Electrical Power
ESFAS	Engineered Safeguards Features Actuation System/Signal
FY	Fiscal Year
HACS	Human Action Classification Scheme
HPIP	Human Performance Investigation Process
HRA	Human Reliability Analysis
HSECS	Human-System Event Classification Scheme
HSI	Human-System Interface
IAEA	International Atomic Energy Agency
IIT	Incident Investigation Team
INEL	Idaho National Engineering Laboratory
INSAG	International Nuclear Safety Advisory Group
IPE	Individual Plant Examination
LER	Licensee Event Report
LOCA	Loss of Coolant Accident
LOSP	Loss of Offsite Power
LP&S	Low Power and Shutdown
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
PORV	Pilot/Power Operated Relief Valve
PRA	Probabilistic Risk Assessment
PSF	Performance Shaping Factor
PWR	Pressurized Water Reactor
RCS	Reactor Coolant System
RES	NRC Office of Nuclear Regulatory Research
RHR	Residual Heat Removal
RV	Reactor Vessel
SCG	Senior Consulting Group
SNL	Sandia National Laboratories
TMI-2	Three Mile Island Unit 2
UAC	Unsafe Act of Commission
UAO	Unsafe Act of Omission

1. INTRODUCTION

1.1 Background

Since the early 1970s, human reliability analysis (HRA) has been considered an integral part of probabilistic risk assessments (PRAs). Although various approaches and methods have been used since the first HRA was performed two decades ago, as part of the Nuclear Regulatory Commission (NRC) sponsored Reactor Safety Study (WASH-1400), the technology associated with HRA is still not fully developed. Better integration of HRA into the PRA process has long been a recognized NRC concern. For instance, the review of the NUREG-1150 severe accident risk PRAs, particularly the comments by the special review committee chaired by Herbert Kouts, Ph.D., pointed out various deficiencies in the HRAs of those NRC-sponsored PRAs. In its response to the Kouts Committee review, the NRC Staff stated in Appendix E of NUREG-1150 (January 1991), that "...the demonstration and more widespread use of improved HRA methods in PRA is planned to be the subject of future work by NRC..."

The limitations of existing HRA approaches become apparent when the role of the human is explicitly examined in real nuclear power plant (NPP) events. Severe NPP accidents and recent NRC studies, such as NUREG-1275 and -1449, indicate that human performance is a dominant source of risk for all modes of plant operation, i.e., low power and shutdown (LP&S) and at-power. Severe accidents during power operation, namely Three Mile Island Unit 2 (TMI-2) and Chernobyl Unit 4, significantly involved management, operations, and maintenance personnel. Details of the implications of human performance related to these severe accidents are given in Kemeny (1979) and Rogovin et al. (1980) for TMI-2, and in NUREG-1250 and -1251 for Chernobyl Unit 4. Also significant human involvement in LP&S events were documented in, for example, Diablo Canyon Unit 2 in April 1987 (NUREG-1269), Vogtle Unit 1 in March 1990 (NUREG-1410), and Prairie Island Unit 2 in February 1992 (NRC/AEOD Human Performance Study Report and NRC/Regional Augmented Inspection Team Report). All these LP&S and at-power events involved human errors of commission (e.g., actions performed which initiated the event or complicated its recovery). Currently, HRA methods and techniques are not specifically designed to adequately account for these types of human actions and do not support their integration into the PRA.

As documented in NUREG/CR-6093 (Barriere et al., 1994b), interest in improving HRA modeling intensified several years ago (1991) when the NRC/RES-sponsored PRAs for LP&S modes of operation were undertaken. NRC/RES recognized that the development of new or improved HRA methodologies were needed to better represent human performance and to increase the utility of PRAs to more realistically represent the risk associated with all modes of plant operation. To accomplish this objective, an improved HRA project (NRC JCN L-2415) was started in February, 1992, at Brookhaven National Laboratory (BNL).

The purpose of the BNL project, entitled "Improved HRA Method Based on Operating Experience," is to develop a new method for HRA based on the analysis of risk-significant human performance in real NPP events. This approach will allow a more realistic assessment and representation to be made of the human contribution to plant risk during all modes of operation. Also, it is important that the new HRA method be fully integrated with PRA. As shown in Figure 1.1, the project's completed, ongoing, and future efforts are divided into four phases:

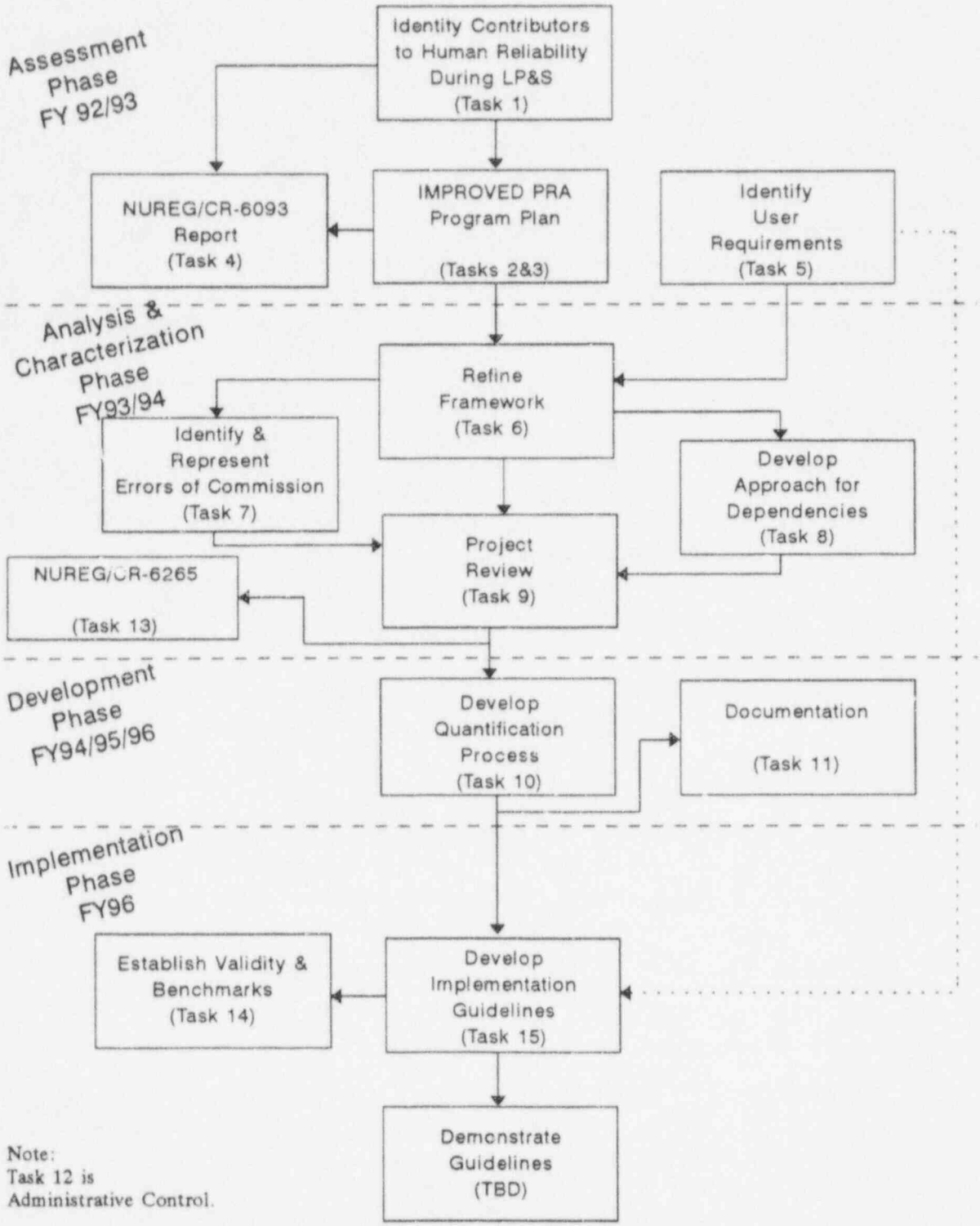


Figure 1.1 Improved HRA project program plan flow diagram

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

The research in the Assessment Phase began by examining events during LP&S. Certain special conditions during LP&S led to questions regarding the ability of current HRA methods to represent salient issues, including a heavy reliance on manual actions with limited procedural guidance and the limited availability of alarms and instrumentation.

The Assessment Phase was of a joint effort between BNL and Sandia National Laboratories (SNL) to make a focused evaluation of human performance in significant LP&S events. BNL evaluated events occurring at pressurized water reactors (PWRs), while SNL evaluated events at boiling water reactors (BWRs). A Human Action Classification Scheme (HACS) was developed for categorizing human actions and associated influences in actual LP&S events. A review of events reported in Licensee Event Reports (LERs), NRC Regional Augmented Inspection Team (AIT) and Headquarters' Incident Investigation Team (IIT) reports, and NRC/AEOD Human Performance reports identified the risk significance of errors of commission (EOCs), human dependencies, and multiple performance shaping factors (PSFs).

Findings from the Assessment Phase suggested that the relevance and importance of specific human-reliability influences can differ from plant to plant for various events and event sequences. Consequently, the specific applicability of what we learn from continued HRA research efforts may be plant-and event-sequence specific, rather than operating-mode specific. Furthermore, the increased understanding of the causes of human errors should be relevant to all modes of operations to improve the modeling and quantification of human performance. We judged that HRA methods developed for LP&S can, and should be, applied to at-power operations to clarify key issues and to permit modeling of those human interactions most important to risk. Therefore, our efforts were expanded to incorporate the analysis of human reliability issues for at-power operating modes.

Recognizing that both current at-power and LP&S PRAs did not thoroughly account for EOCs, human dependencies, and the influence of plant conditions and multiple PSFs, an outline of a program plan was developed to address these observations and improve HRA and its integration with PRA, for all modes of operations. The outline also identified the requirement for a multidisciplinary HRA framework to describe the relationships among human factors, behavioral science, and plant engineering and operations within a PRA context. The framework would support the further analysis of operational data, guide improvements to human error modeling, and provide the basis for integrating the HRA quantitatively into the PRA.

The accomplishments of the Assessment Phase (including details of the BNL and SNL parallel efforts and the program plan outline) were documented in NUREG/CR-6093, "An Analysis of Operational Experience During LP&S and A Plan for Addressing Human Reliability Assessment Issues" (Barriere et al., 1994b).

The Analysis and Characterization Phase of the project, the subject of this report, consisted of the following activities:

(1) the development of a multidisciplinary HRA framework for improving the integration of HRA with PRA;

(2) the characterization of EOCs and human dependencies, including general guidance for their identification and representation in PRAs; and

(3) an independent peer review of the project's accomplishments, to provide suggestions for modifications, and recommendations for further developments.

Figure 1.1 illustrates the relationships between these activities and the other project tasks. The results of these efforts, including research implications, development requirements, and future plans, are discussed in Sections 2 through 8, and Appendices A through C.

1.2 Objectives

This report meets the following objectives:

(1) Documents the overall HRA framework and approaches for characterizing EOCs and human dependencies, accomplished during the Analysis and Characterization Phase,

(2) Summarizes the results of the February 1994, Independent Peer Review of the Analysis and Characterization Phase, and

(3) Discusses research insights and necessary further research activities required for the project's Development and Implementation Phases.

1.3 Outline of the Report

Figure 1.2 shows the structure of this report. The background and objectives are identified in this section. The motivation for improving HRA and PRA is discussed in Section 2, which establishes the importance of this work by noting that certain kinds of human error play a prominent role in major technological disasters, and they are not well modeled in current PRAs.

Sections 3, 4, and 5 summarize the results of the Analysis and Characterization Phase in terms of the HRA Framework, EOCs, and Dependencies. These topics are described further in the individual task reports in Appendices A *(Refined Human Reliability Analysis (HRA) Framework)*, B *(Identification and Representation of Errors of Commission (EOCs))*, and C *(Develop Approach to Deal with Human Dependency)*, respectively. While the task reports provide more detail than their respective section summaries, they were originally produced in January 1994 in support of the Independent Peer Review process. In some instances the section summaries reflect an update to these original task reports.

Section 6 documents the independent peer review, and Section 7 defines the research implications of the work. Section 8 discusses future plans and potential regulatory applications. Section 9 cites the references used in the report.

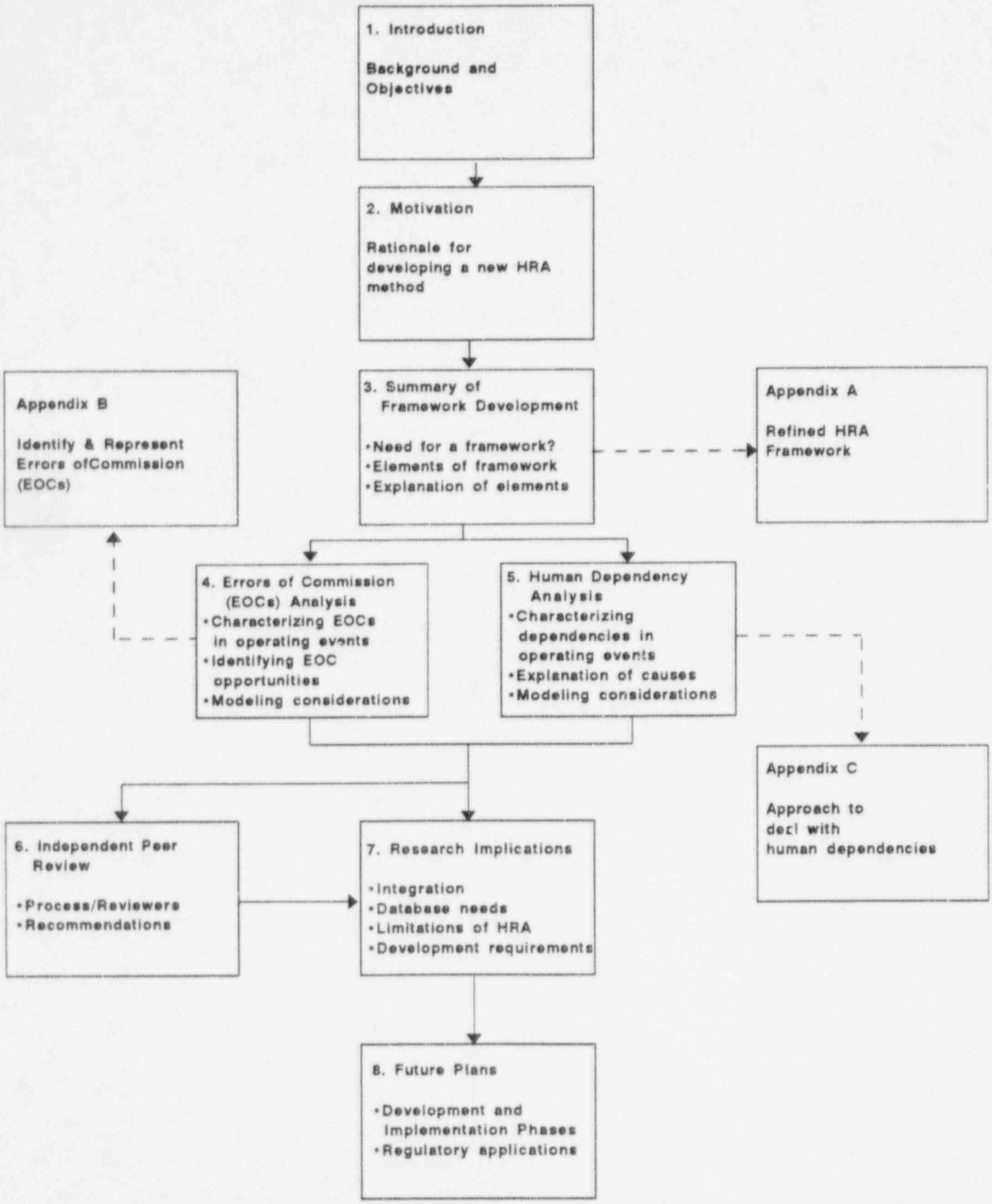


Figure 1.2 Structure of the report

2. MOTIVATION FOR IMPROVING HRA/PRA

Human operators monitor and control the operations of nuclear power plants (NPPs). During off-normal or accident conditions, they must ensure that the automatic systems needed to maintain safety are operating or they must manually intervene. Consequently, humans are involved when safety is challenged and, when safety barriers fail, human error is commonly a key ingredient. The human reliability implications of these contributions are a prime area of investigation in this project.

Morey and Huey (1988) reported that errors caused by operators in the control room were a significant contributing factor to NPP accidents, such as the 1979 Three Mile Island Unit 2 (TMI-2) accident. The International Nuclear Safety Advisory Group (INSAG) of the International Atomic Energy Agency (IAEA) found that one of the most important lessons learned from incidents, ranging from minor to severe accidents, is that they are often the result of incorrect human actions (INSAG, 1988). Furthermore, they claim that a vital component of defense-in-depth is the operating staffs' "...continued knowledge and understanding of the status of the plant..." This contribution of human errors is not unique to the nuclear power industry. Descriptions of accidents at chemical process facilities (e.g., Kletz, 1985) and in commercial aviation operations (e.g., NTSB/SS-94/01) indicate a large contribution from human errors. For example, almost 70% of all accidents involving commercial jet aircraft are caused by cockpit-crew errors (Nagel, 1988).

There has been a growing recognition that existing HRA methods do not realistically represent the roles humans play in preventing, initiating, and mitigating NPP accidents. Examples of these concerns were presented in a special HRA issue of "Reliability Engineering and System Safety", and introduced in a challenging guest editorial by Dougherty (1990). Other examples were documented by Parry and Lydell (1991) and Wreathall and Reason (1992), and discussed during several international workshops (e.g., Post-SMIRT, 1988, and Stockholm, Sweden, 1994). The general nature of these criticisms is that current HRAs, and, as a consequence PRAs, do not fully represent human performance and reliability as observed in actual operating events.

Most notable is the concern that HRA methods cannot adequately address, or accommodate, the underlying causes of severe accidents. Furthermore, these underlying causes often involved human errors of commission (discussed in Section 4), multiple dependent actions that span the temporal phases of an accident (discussed in Section 5), and new plant states created by human-system interactions. This lack of consideration is due, in part, to the fragmented development of HRA methods (e.g, some concentrating on only the immediate post-accident diagnostic phase, and others only considering a limited set of human error mechanisms and performance-shaping factors), as well as overly simplistic modeling and probability estimations. Consequently, the contribution of human reliability to real accidents is not sufficiently represented in current PRAs.

As discussed later, reviews of the severe accidents at Chernobyl, TMI-2, and elsewhere indicate that human reliability plays a more significant role than that reflected by human errors typically modeled in current PRAs. Errors, such as omitting a procedural step, selecting an incorrect switch, or failing to initiate a safety-related function, are the typical human failure modes represented in many PRAs, for example, NRC-mandated Individual Plant Examination (IPE) studies. This limited type of modeling is largely due to constraints imposed by current HRA methods.

2.1 Real Accidents

On April 26, 1986, the Chernobyl Nuclear Unit 4 suffered the worst accident in the history of commercial nuclear power. Early reports on the accident indicated that plant operators took extraordinary chances during an experiment. The international community was told that the Russian RBMK reactors were quite safe if operated according to well-established procedures. This accident was stated to be simply a case of "pilot error," in which the error bordered on criminal irresponsibility (INSAG-1, 1986). In fact, several plant managers subsequently were sent to prison for their roles in the accident.

Following the accident; however, additional events unfolded, which changed the picture initially presented by the Soviet government. The respected academician Valeri Legasov, who gave the initial report to the international community, committed suicide. Apparently upset by the presentation in Vienna, he left behind a memoir damning the reactors he helped design. These reactors had characteristics never fully understood by the operators which made their control very difficult, if not impossible under certain conditions. In a book, the physicist Grigori Medvedev, while faulting the operators, made it clear that the inherent design had difficult control problems, and only the most brilliant, cool-headed expert could have had a chance to control the situation that had evolved in late April, 1986. Similarly, an earlier review (Nuclear Power Corporation Limited, 1976) determined that the RBMK control system was inadequate in meeting United Kingdom safety criteria.

The initial response from western engineers was that little was to be learned from the Chernobyl accident of direct relevance to western reactors. Unlike western reactors, the Soviet RBMK design was seen as inherently unstable. Increasing the power and coolant-voiding drove power even higher, spiraling upwards to eventually destroy the core. By contrast, western reactors were designed to be self-limiting, increasing fuel temperature promptly shuts down the chain reaction (this is usually enhanced by the resultant increase in coolant temperature as well). Because a reactor like Chernobyl would never be built in the west, it was thought that the accident taught us little, save that we were aware of the importance of designed-in safety.

In 1991, following the dissolution of the USSR, Piers Paul Read gained access to records and individuals not previously known to the West. Read (1993) describes a system almost guaranteed to result in an accident. The IAEA International Nuclear Safety Advisory Group revisited the record in 1992 and reached similar conclusions (INSAG-7, 1992).

In trying to abstract the bare essentials of what happened at Chernobyl from the accident records, a series of three conditions related to the operators' performance can be identified that had a significant impact on the accident:

(1) the operators intentionally violated the rules on power and reactivity requirements;

(2) the plant then entered an unusual regime where the core physics were not understood; and

(3) the operators continued to refuse to believe the evidence coming to them, both from instrument readings and eyewitness reports.

The implications of this sequence of events is especially troublesome to the West when the TMI-2 accident of March 29, 1979 is considered (Kemeny, 1979, and Rogovin et al., 1980). Having reframed

the Chernobyl accident in terms of human interactions identified above, a striking parallel with TMI-2 becomes apparent. At TMI-2, the following events occurred:

(1) the plant was operated with a leaky pressurizer power-operated relief valve (PORV) and in violation of the requirements for emergency feedwater (EFW) availability with two EFW block valves closed and disabled. In addition, actions taken to clear a condensate-resin blockage initiated a loss of main feedwater, and led to the subsequent sequence of events.

(2) the plant then entered an unanticipated regime where the indications and implications of the reactor coolant system (RCS) reaching saturation were not understood.

(3) alternative rationalizations were developed to explain the instrument readings that should have shown the true status of the reactor.

Thus, the two worst accidents in the history of commercial nuclear power share similar sequences of human interactions. By focusing on the detailed sequences of events and peculiar design aspects of each accident, this common thread can been identified. Its implications in terms of their representations of the characteristics of severe accidents are discussed next.

2.2 Characteristics of Severe Accidents

When the conditions described above are generalized slightly they can be restated as three characteristics of severe accidents:

(1) the plant is operated outside the designer's intentions;

(2) the plant then enters a regime where its behavior is not understood; and

(3) the operators fail to recognize, or refuse to believe accumulating evidence.

With this "reframing" in mind, similar sequences of human interactions can be found in many of the LP&S events analyzed in the project's earlier phase (reported in NUREG/CR-6093). Moreover, recent discussions with those who have analyzed transportation and aviation accidents and reviews of accidents at chemical plants (e.g., Kletz, 1985) suggest that these types of interactions often occur in serious accidents involving human operational control for these industries. Significantly, such human interactions are not well modeled in existing PRAs. While never stated explicitly, this observation may be a source of some distrust about PRAs; e.g., that human error is a dominant contributor to risk, and that instrumentation problems also are important, but their risk impact is not reflected in current PRAs. This inadequate representation is a strong motivation to develop new and better HRA and PRA methods. The ability to incorporate these types of characteristics into a PRA is a major goal of this project as it moves into the HRA method Development Phase.

The observations of these characteristics followed the research on human EOCs and dependence mechanisms (defined in Sections 4 and 5, respectively), based on a new perspective gained from analyzing and characterizing operating event histories using the multidisciplinary HRA framework (to be described in Section 3). Reframing the Chernobyl and TMI-2 accidents from this point of view allowed the project team to formulate the connection between seemingly diverse sequences of events.

In the language to be developed and defined in Sections 3 through 5, operating outside the designer's intentions can create an unanalyzed plant condition that is beyond normal operator training and/or procedures, which then can activate a human error mechanism related to, for example, inappropriate situation assessment (i.e., a misunderstood regime). This then can result in a refusal to believe evidence that runs counter to the initial misdiagnosis, subsequent errors of commission, and ultimately, an accident with potentially catastrophic consequences.

The three characteristics are not intended to represent the only mechanisms for a severe accident. Other sequences of events can be hypothesized to lead to severe consequences, as PRA have identified. However, the two most serious accidents in commercial nuclear power share these characteristics, along with many serious accidents in other industries. If PRAs do not identify such events, it is important to ask why. The answer would appear to be that PRA analysts have not been looking for this category of accident sequence.

Of the three characteristics, the first requires additional exposition. The reasons for operators taking the plant outside the designer's intentions can happen for several reasons:

(1) *The intentions are not well thought out by the designer.* "The designer" represents the entire design and analysis team of the vendor, architect/engineer, utility, and regulator. If the wide range of possible conditions that can occur are not analyzed and at least bounded by the designer a priori, the operators cannot fully understand the implications of their actions. Therefore, the operators must understand what conditions have been analyzed so that they can avoid those uncertain, unanalyzed conditions.

(2) *The intentions are not well communicated to the operators.* The extent of the design analysis, the range and applicability of procedures, and the possible consequences of straying from known territory must be conveyed to the operators through training programs and procedures. Because no procedure can be complete and cover all possibilities, training must instill the knowledge and judgement to permit wise, flexible use of procedures, as shown by Roth et al. (1994).

(3) *The intentions are ignored by the operators.* This can happen through minor slips or, more seriously, through erroneous intention. The latter often occurs for seemingly good reasons and is not malicious, but can be troublesome when based on invalid experience (generalizing from a superficially similar experience), or inadequate knowledge of the range of the plant's analyzed performance.

(4) *Bad procedures direct operators to take the plant outside the designer's intentions.* Procedures can be inadequate for many reasons. They may be developed for a unique situation and inadequately tested. For example, they may be based on a specific case, identified by design analysis, that does not quite apply to the real scenario in the plant.

These insights on the three characteristics are relatively new, having been uncovered towards the conclusion of the project's recent Analysis and Characterization Phase. The details of including them in the framework, and methods for identifying them and their potential influence on vulnerable plant conditions are under development. The following section discusses further evidence on their contribution in severe accidents.

Further Examples of the Three Characteristics of Severe Accidents

In addition to the TMI-2 and Chernobyl severe accidents, the three characteristics also have been found in the records of, for example, the Challenger space shuttle accident (Challenger Accident, 1986), the misadministration of medical radioisotopes at Indiana, Pennsylvania (NUREG-1480, 1994), and the crash of the Air Florida 737 aircraft (Wreathall, 1990). Analysis of detailed event reports describing these accidents identified that, initially, humans performed unsafe actions (operations) that were outside the designer's intentions (i.e., beyond the design basis). These operations were often described in retrospect as having been done for what was perceived to be a good reason or with good intentions, e.g., "it's the only way to do the job," "it's the only way the system works in practice," or "that's the way we always do it."

Under rare but significant circumstances akin to each accident, the consequence of the initial unsafe actions led the system into a condition (regime) that was not fully understood or apparent. The following are some examples of misunderstood conditions:

- RCS saturation (TMI-2)
- reactivity changes (Chernobyl-4)
- low-temperature performance of seals (Challenger)
- effects of special conditions on ice formation on aircraft (Air Florida)

After the initial unsafe action and the misunderstanding of physical conditions, the third significant characteristic was the dismissal of evidence indicating the correct status of the system, or the inability to comprehend that the information, in fact, was feedback which could have prevented the accident. This characteristic results from an erroneous mindset creating an invalid alternative explanation, and the subsequent refusal to believe evidence that ran counter to the explanation. Examples of this characteristic included:

- instrument readings dismissed as erroneous (TMI-2, Chernobyl)
- dismissal of credible reports as being incompetent ones (Chernobyl and Challenger)
- instruments ignored or overlooked (Air Florida)

Without incorporating these observed characteristics, a PRA only partially reflects the causes of risk. Consequently, it lacks particular sequences that often are present in the worst technological accidents. Identifying these characteristics is a first step to correcting this limitation.

By extending the multidisciplinary HRA framework developed for this project (described in Section 3) and by analyzing and characterizing additional operating events, the HRA project team anticipates being able to focus directly on these three characteristics. The ensuing development phase of the project will define how to model and quantify them in terms of human responses and influences (e.g., EOCs and dependencies), opening an area of major importance to the risk-management contribution of PRA.

2.3 PRA Perspective

The fundamental motivation for this work is to improve PRAs by closing the gap between current HRA models and the real-world experience of severe accidents. Many previous projects, sponsored both by industry and the NRC, have had similar goals, and many have made improvements, though usually only in to one or two aspects of the problem within a single discipline, such as PRA or human factors. By

using our new multidisciplinary HRA framework, knowledge from many diverse disciplines can be synthesized. The intention is to address previously neglected HRA and PRA issues by expanding the boundary of what HRA can model and quantify, and providing a depth of realism in PRA that previously was impractical.

Improving the realism of PRA by improving the modeling and quantification of human performance has been a major goal throughout the project. Early on, we recognized that current HRA methods (for both full power and LP&S) cannot adequately cover many observed human actions, specifically human-induced initiators and post-accident mistakes, as well as their associated EOCs and dependency implications. HRA modeling must be improved to rectify the mismatch between real events and PRA analyses. For example, many people in the nuclear power industry feel that it is important for PRA to be able to predict such events as TMI-2 and Chernobyl. In both events, human actions played an important role in the progression of the accident. Furthermore, the safety significance of these human actions appears to be understandable only in the context of the specific circumstances at the time of the events (e.g., plant conditions, system configurations, PSFs), limiting the ability of current HRA methods to predict these actions. To identify the circumstances and predict their influence on human actions, improvements to HRA must consider the diverse disciplines of engineering, human factors, and the behavioral sciences, as well as PRA.

PRA is unique among the disciplines that relate to safety in that it defines safety in integrated, quantitative terms using accident sequences, including initiating, hardware, and human events, and the specific outcomes of those sequences. Depending on the level of the PRA conducted; i.e., Level 1, 2, or 3 for NPPs, the outcomes calculated are core-damage frequencies, release frequencies, and expected fatalities and early cancers, respectively. The PRA model connects these outcomes and their causes (i.e., the initiating events plus combinations of hardware and human failures).

PRA relies on existing knowledge of physical phenomenology, engineering principles, and experience to build appropriate models. In and of themselves, disciplines other than PRA cannot provide an integrated connection to consequences for public safety. For example, human factors engineering does not include methods that demonstrate how labeling practices specifically translate into some significant measure of difference in NPP safety. Similarly, issues such as safety culture, staffing, and overtime have impacts on certain types of human performance, but their quantitative connection to important public safety concerns (e.g., increased probability of early cancer for the nearby population) has not been demonstrated. This connection between calculated consequences and model inputs is an important strength of PRA, i.e., to identify risk-significant events (human, hardware, external) and their associated safety implications.

Therefore, the challenge is to develop PRA models, specifically HRA models, that reduce uncertainties in the calculated consequences to public health and safety. Credible models used in the HRA portion of the PRA will account for the information in the behavioral science literature on the major contributors to human-error, and will provide a mechanism to translate those contributors and the resulting estimated human error probabilities to consequences for public safety. An important goal of the human factors disciplines in PRA (similar to the roles of the other scientific and engineering disciplines) is to expand the scientific knowledge of those factors which impact the performance of hardware and humans, and define the nature of their impact. PRA models then will continue to be improved to accommodate developments in scientific and engineering knowledge.

Many current PRA analyses were conducted for one specific purpose: to gain a general understanding of a plant's vulnerabilities to core damage under nominal, design-basis conditions. In this regard, PRAs have served the cause of risk management well. They generally represent an average; for example, average plant conditions at the time of an event, component and system reliabilities averaged over several years, or the response of an average operating crew. However, with their techniques and underlying definitions of risk, PRAs can be refined for any number of objectives, including improving our understanding of the risk significance of human performance.

Certainly, expanding PRAs to understand the risk significance of human performance can be accommodated. This will involve modifying PRA assumptions and typical modeling conventions that reflect "nominal" conditions, to expand and investigate the safety concerns represented by the special circumstances surrounding events such as TMI-2 and Chernobyl.

2.4 Motivation Summary

In developing an improved HRA method that is based on operating experience, and in providing a modeling and quantification approach that is fully integrated with PRA, we soon recognized the need for a multidisciplinary framework (reported in NUREG/CR-6093, and discussed in Section 1). To achieve a fundamental goal of incorporating into PRAs those human actions observed in real accidents with severe consequences, the framework can provide a way to structure what we know about NPP safety, human performance, and the underlying factors that affect them. The framework must be multidisciplinary because the factors affecting human reliability and plant safety are based in many sciences. By bringing together those different languages and ideas among disciplines, the framework can clarify perceived conflicts and promote mutual understanding. Hence, the specific purpose of the framework is to provide a structure for analyzing operating experience and integrating insights from the human factors, behavioral science, plant operations, and engineering disciplines into the PRA process.

With the insights obtained from the framework, we anticipate that the improved HRA modeling and quantification approach will allow us to identify and incorporate important causal factors of human errors (e.g., errors of commission) consistent with operating experience, to model the interrelationships between those factors, to estimate their impact on human errors, and to produce a quantitative estimate of human error at the level required within the HRA/PRA process. In addition, there are important user-and traceability-related issues, such as the need for more practical guidance, and simple operational definitions of PSFs and plant conditions, for example. Addressing these issues will help assure that human reliability considerations can be effectively incorporated into the PRA.

Accordingly, the project's Analysis and Characterization Phase set out to (1) develop a multidisciplinary framework, (2) develop an approach for quantifying and modeling EOCs, and (3) develop an approach for assessing dependencies between human actions. The following sections discuss our accomplishments and identify the improvements needed to integrate them into an improved HRA/PRA process.

3. MULTIDISCIPLINARY FRAMEWORK DEVELOPMENT

3.1 Introduction

In recognizing that existing HRA methods do not represent realistically the roles of humans in the initiation, prevention, and/or mitigation of accidents at nuclear power plants (NPPs), formalized descriptions are needed for the relationships between human actions, associated errors, and the influences of performance shaping factors (PSFs) and plant conditions on human reliability. Therefore, a critical task of this project was to develop a multidisciplinary HRA framework that defines these relationships. With this basis, we subsequently can explore the issues associated with errors of commission (EOCs) and dependencies between multiple human errors, and can provide a foundation for considering ways to model and quantify human errors in PRAs more realistically.

Figure 3.1 is a graphic description of the framework, illustrating the interrelationships between unsafe human actions, their influences on the plant, and the influences of the plant and PSFs on human reliability. The framework is multidisciplinary, including 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. This framework emerged from the review of significant operational events at NPPs by a multidisciplinary project team. The elements included are the minimum necessary set to describe the causes and contributions of human errors in the major NPP events described earlier.

The HRA-related elements; e.g., human factors, behavioral science and plant engineering disciplines, are reflected on the left side of the figure, namely PSFs, plant conditions, and error mechanisms. These elements represent underlying causes (i.e., influences) of human errors; hence, they explain why a person may perform an unsafe action (to be defined later). The unsafe action element represents the point of integration between the HRA and PRA (denoted in Figure 3.1 by the dashed vertical line that runs through its center). The elements on the right side of the figure represent the PRA perspective with which the HRA-related elements ultimately must be integrated. PRAs traditionally focus on the consequences of the unsafe action, which they describe as a human error represented by a human-failure event. The human-failure event is included in the PRA model for the applicable plant state(s). The specific accident scenarios that the PRA model represents are defined by the plant state.

Appendix A describes the development of this multidisciplinary framework in more detail and compares it with the implicit framework often used for current HRA/PRA integration. The following sections are a detailed summary of each element and their interrelationships (illustrated by the arrows in Figure 3.1). An example of its application and some conclusions about its potential use and expansion also are discussed.

3.2 Elements of the Framework

This section summarizes the principal elements and relationships of the framework and why they are important for understanding the human contribution to safety and for representing human errors in PRA modeling. The concepts and terminology are briefly illustrated in Section 3.3, and more completely described in Appendix A with an example of an event that occurred at a U.S. commercial NPP (Prairie Island Unit 2, 1992).

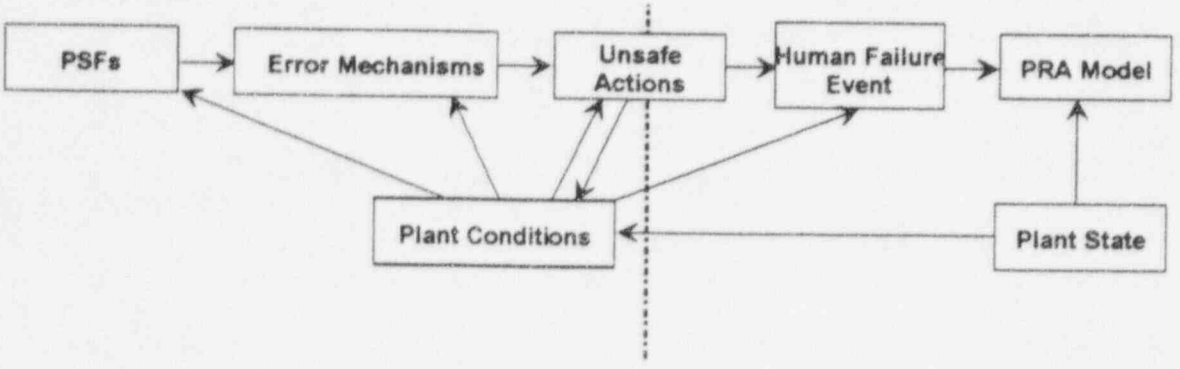


Figure 3.1 Multidisciplinary HRA Framework

3.2.1 PRA Model and Plant State

The PRA model and plant state elements shown in the framework (Figure 3.1) are equivalent to those used in existing PRA methodologies. For developing improvements in HRA, the PRA model is considered an "end-user" of the HRA process.

The PRA model assesses the risk associated with NPP operation as a function of human failures and equipment unavailabilities. It is comprised of logic models that identify and estimate the frequencies of event scenarios that lead to accident scenarios, and the various failure modes of the between equipment and humans that are required to respond to the initiating event. The model estimates the frequencies of such scenarios by converting the logic model into a probability model.

The building blocks of the PRA logic models are "basic events" that include different failure modes of components and subcomponents which, in combination, lead to failures of systems. The basic events are combined in the logic models as fault trees and event trees according to the definitions of system and functional failures. Combinations of fault trees are represented in the PRA event trees according to the plant state being analyzed (such as a loss-of-coolant-accident [LOCA], loss-of-offsite-power [LOSP], or another accident scenario) to describe combinations, i.e., accident sequences, that lead to unacceptable accidents such as core damage.

When human performance issues are analyzed to support PRA, it is in the context of the accident scenario defined by the plant state and represented by a PRA logic model. The final HRA quantification is typically performed on a "cutset-by-cutset" basis; for example, when post-accident responses are quantified based on the timescale available for action. Cutsets are unique combinations of basic events that define an accident, which result from the Boolean logic represented by PRA event trees and fault tree models. One cutset may represent a combination of hardware failures associated with a pump in one train and a valve in another train, and failure of the operators to recover operation. Another cutset may represent human-caused failures of the same pump and valve, together with failure of the operator to recover either the pump or the valve. The ability of the operator to recover the plant from human-caused

failures may differ from the ability to recover from hardware failures because of dependencies between the human actions causing equipment to fail and the potential recovery actions. Consequently, these differences should be reflected in the PRA model.

3.2.2 Human Failure Events

The human failure event element depicted in Figure 3.1 refers to a specific type of basic event in a PRA logic model involving the loss of a function or system availability, or an equipment failure due to an unsafe human action(s) which places the plant at greater risk. A human-failure event reflects the PRA systems analysis perspective and is defined as either an error of omission (EOO) or an error of commission (EOC). An example of an EOO human failure event is the failure to initiate a required safety function. Examples of EOC human failure events include the termination of a necessary safety function, or the initiation of an inappropriate system.

The reason for using the term "human-failure event" rather than the frequently used term "human error" is that "human error" means many different things to the different disciplines involved in assessing human reliability. "Human error" when used by behavioral scientists often refers to deficient cognitive processes which can be very different from that intended by the PRA analyst, whose concern is that an unsafe condition results. Historically, the cognitive deficiencies associated with "human error" have been of limited concern to PRA. In contrast, from the behavioral scientist's perspective, the systems consequence of the error generally is of limited interest compared with the causes underlying the error. The behavioral sciences aspects of human errors are discussed below.

3.2.3 Unsafe Actions

The unsafe actions element depicted in Figure 3.1 represent those actions by plant personnel inappropriately taken, or not taken when needed, that degrade plant safety. An 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 elaborated in Section 4, there is a distinction between PRA human failure events defined in terms of EOC and EOO, and the operational event-data defined in terms of unsafe act of commission (UAC) and unsafe act of omission (UAO). The UAC and UAO are human actions identified in historical event data that degraded plant safety. How they relate to the PRA representation of a human failure event of an EOC or EOO depends 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.

In some cases, there is a direct correspondence between unsafe actions and human-failure events. For example, operators terminating operation of needed engineered safety features would be a UAC, and should be incorporated as an EOC 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 often are specific to the circumstances in a particular event. For example, in the operational event at Prairie Island Unit 2 in 1992 (NRC/AEOD Human Performance Study Report), the unsafe actions were the erroneous

calculations, which led operators to fail to terminate draindown before suction to the RHR cooling loop was lost. The actual unsafe actions were two rule-based mistakes (defined below) made in calculating level while draining down the reactor coolant system (RCS) and the reactor vessel (RV). However, from the PRA perspective, the human-failure event, defined in the context of the plant state, would be identified as 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 types are slips and lapses, mistakes, and circumventions. The distinction between them is (1) their potential impact on safety differs, and (2) the factors causing each differs. Each type is summarized below.

Slips and lapses are unsafe actions where the outcome was not what the person taking 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 a skill-based level of performance associated with routine highly practiced actions. The significance to risk of these unsafe actions seems to be quite small because these actions, not being as the "actor" intended, are often easily recognized by the person involved and easily corrected (in most circumstances).

For unsafe actions where the action was as intended, there are often 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 demands rule-based or knowledge-based performance. For rule-based performance, documented task-specific instructions are followed (usually in procedures, for almost all NPP activities important to safety); the mistake, therefore, represents an unsafe action performed while following procedural guidance, which is either inadequate or technically correct but not applicable to the current situation (e.g., inappropriately selected based on an erroneous diagnosis). For knowledge-based performance, the person involved is relying on ingrained technical or specialist knowledge (as in generalized troubleshooting); therefore, it represents an unsafe action performed under unusual circumstances while relying on ingrained but deficient technical knowledge without direct procedural guidance.

Mistakes are perhaps the most significant to risk because they are being followed purposefully by a person who may have limited cues that there is a problem based on an erroneous diagnosis. Indeed, indications contradicting the erroneous diagnosis often are dismissed as "instrument errors," for example. In many circumstances, it takes an outsider to identify the type of 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 (while knowing the rule) for what seems to be a good (or at least benign) reason. The intention ignores the known rule, usually based on the perception that the circumvention will have little or no impact on plant safety. For example, maintenance personnel may purposely reverse the steps in a procedure to simplify or shorten a task. Circumventions potentially are significant contributors to risk, in that unanalyzed conditions can result from unexpected combinations of circumventions and other unsafe actions or equipment failures. However, a condition that seems to lessen this potential is that the person committing the circumvention (usually) is aware of it and can take mitigating actions to restore safe operation. Presently, circumventions seem to be rarely reported incidents which may reflect a low rate of occurrence. However, recent simulation tests indicate that they may be quite common (Roth, 1994), but not

considered reportable. Circumventions are distinct from acts of sabotage because they are not intended to cause damage.

3.2.4 Error Mechanisms

Error mechanisms are the cognitive characteristics of human information-processing that influence the performance of an unsafe action (Figure 3.1). They represent different failures in processing information and executing a response that explain why a person fails to take an action or takes some inappropriate action. They include failures in attention, situation assessment, response planning, and response execution. 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 execution failure); second, they may misread the valve number in the procedure or on its identification label (for example, reversing two digits) and open the wrong one (an attention failure); third, the selected procedure may have been the wrong one (a situation-assessment failure); fourth, the operator may perform the steps of the procedure out of their written sequence perceiving that its better to perform the task that way, and consequently, failing to open the valve at the correct time (a response-planning failure). From the safety perspective and that of PRA modeling, the unsafe action for all of these cognitive failures is still "operator fails to open valve."

Different error mechanisms are primarily associated with different kinds of unsafe actions. For example, failures in situational assessment are error mechanisms associated with mistakes, whereas failures in attention are associated with slips and lapses. In consequence, the risk impact of the error mechanisms potentially differ according to the different risk impacts of types of unsafe action.

Error mechanisms are not observable in themselves, only their consequences as unsafe actions can be observed. They serve to explain how the influences of performance shaping factors (PSFs) and plant conditions result in unsafe actions. They are included in the framework because they help to describe why different groups of PSFs and plant conditions are associated with different kinds of unsafe actions and their different importances to safety and risk. By examining these error mechanisms, it is possible to identify the combined influence that PSFs and plant conditions have on unsafe actions. The HRA method we are developing will include ways to search for these potential error mechanisms and to represent them in definitions of human failure events for PRA.

3.2.5 Performance Shaping Factors

PSFs influence the occurrence and type of human error mechanisms during operations, testing, and maintenance (Figure 3.1). In Swain's original (1967) work (reported in Swain and Guttmann (1983)), a PSF was defined as "any factor that influences human performance." Such a broad interpretation has become narrowed in the practice of HRA to refer to specific features of the human-system interfaces. In these authors' Technique for Human Error Rate Prediction (THERP), these interfaces include such features as the layout and types of displays, the format of procedures, labeling of components, and administrative controls (such as checking). In other methods, PSFs have been related to the timescales of accident conditions and the availability of training (e.g., simulator training).

With the differences between the possible error mechanisms that could cause an unsafe action, using a single set of PSFs for all types of mechanisms and unsafe actions is inappropriate. Rather, each error mechanism has an associated primary set of PSFs. Table 3.1 identifies some basic relationships between error mechanisms and sets of PSFs.

To date, the PSFs primarily used in this project are those identified in the Human Performance Investigation Process (HPIP) (Paradies et al., 1993) pertaining to procedures, training, communications, supervision, staffing, human-system interface (HSI), organizational factors, as well as to 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.

Table 3.1 Primary PSFs Associated with Each Error Mechanism

Error Mechanisms (Failures in)	Examples of PSFs
Attention	Workload, Stress, HSI (instrument displays), Environmental Conditions
Situation Assessment	Training, Procedures, Communication
Response Planning	Training, Procedures, Supervision
Response Execution	HSI (e.g., controls layout), Procedures, Communication

3.2.6 Plant Conditions

Plant conditions are the specific features of the plant and its operating state that govern not only the tasks performed, but also the circumstances under which they are performed. With respect to the other elements depicted in Figure 3.1, plant conditions represent influences related to operating configuration and process parameters including equipment/instrumentation availability, the core's reactivity, and the temperature, pressure and inventory of the reactor coolant system (RCS). Particular examples of plant conditions include at-power operations with certain equipment or instrumentation (e.g., displays) failed or otherwise unavailable, and shutdown operations with alarms out of normal operating range and many automatic controls and safety functions disabled. Consequently, plant conditions define the context for the required kinds of human actions, as well as the types of errors that can occur. For example, operations during a PWR refueling outage (such as draining to midloop) requires many manual actions by operators (often under conditions of limited indications and alarms), whereas maintaining a reactor during full power requires only a few manual actions (such as undertaking 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 traditionally defined in the PRA, especially those that could lead to initiating events or other EOCs (e.g., those in the post-accident phase).

A particular feature of plant conditions is the performance history of equipment and instrumentation (e.g., a leaky PORV, a frequently false-positive radiation monitor, or some other equipment with an inherent design problem). Such history was found in operating experience to influence human reliability in both the initiation and response to an event (e.g., at TMI-2). In addition, most difficulties in human performance were found to occur when an activity or task is being performed under unanalyzed abnormal conditions, rather than the design-basis conditions typically used, for example, in task analyses by human factors engineers. The abnormal conditions then render the normally adequate instrumentation and human-factors design features (e.g., PSFs related to training, procedures, and HSI) inadequate or even misleading. These aspects of plant conditions play a significant role in determining the type and

occurrence of unsafe actions; however, they are not explicitly represented in definitions of PRA accident scenarios.

A detailed description of plant conditions is necessary to identify those possible situations, i.e., abnormal conditions, where people are almost forced into failure. For example, in the loss of residual heat removal (RHR) event at Prairie Island Unit 2, in February 1992, the combination of PSFs associated with workload, ambiguous task requirements or instructions, inexperienced and under-trained personnel, and a lack of supervision, together with plant conditions associated with nitrogen overpressure in the RCS caused the operators to overdrain the RCS water level below midloop within 48 hours of shutdown. At this time, the decay-heat level still was sufficient to cause boiling in the reactor core within 21 minutes of the loss of cooling flow.

This example indicates the level of specification for plant conditions that must be considered to define the conditions under which people can fail. In addition, this level of description allows the identification of risk significant EOCs since they primarily result from errors during periods of intervention with the plant (such as changing power levels, performing surveillance testing, or during LP&S operations). Section 3.3 gives a fuller evaluation of the Prairie Island event in terms of the framework.

As Figure 3.1 illustrates, plant conditions impact many of the other components of the framework: PSFs, error mechanisms, unsafe actions, and human-failure events. These influences are summarized below.

Impact on PSFs

Many of the PSFs depend on the plant's condition. For example, consider the differences between LP&S and at-power operations. Procedures are often less valid for LP&S. Instrumentation often is different for LP&S, such as the RCS level being read from a tygon tube rather than the installed RCS level-measurement system. Training is different; for example, simulator-based training of operators for LP&S conditions is very rare. Even under at-power operations, there can be differences between PSFs for different classes of accidents as would be represented by the plant states modeled in PRA.

Impact on Error Mechanisms

Plant conditions impact error mechanisms by creating a context which determines the sensitivity of plant personnel to particular PSFs, thereby providing the opportunity for error mechanisms to occur and result in unsafe actions. For instance, the plant conditions at the task level (e.g., performing maintenance on a particular valve, or draining the reactor water level to midloop in a PWR within several days following shutdown) provide specific opportunities for error mechanisms to arise. Maintaining a particular valve may require considerable attention to very fine details in the setup, as with a suction relief valve (e.g., 1989, Braidwood Unit 1 event). In that activity, significant opportunities for errors associated with, for example, recognition or attentional failures can be presented that would not be part of the maintenance of mechanically simpler valves. Similarly, during that valve maintenance task, deficiencies in PSFs such as lighting and clarity of procedures become more important in influencing the probabilities of error mechanisms. Consequently, plant conditions determine the sensitivity of error mechanisms to particular PSFs, and provide opportunities for manifesting error mechanisms.

Interactions with Unsafe Actions

Plant conditions provide the setting in which the occurrence of an error mechanism results in a specific unsafe action. For example, suppose a failure in attention results in skipping a step in a procedure; the ensuing unsafe action depends on the instructions that were skipped. They were associated with undertaking some time-critical recovery action in the post-accident phase. The unsafe action would be the failure to activate the components listed in the procedure. This would be considered a PRA human failure event due to the potential of contributing to the frequency of core damage as modeled in the PRA. However, if the step omitted was to reconfirm a previously identified alarm condition, then the same error mechanism may have no direct unsafe consequences, and therefore, would not be considered in the PRA. In other words, the same error mechanism may lead to very different unsafe actions depending on the plant conditions.

Alternatively, unsafe actions themselves can change plant conditions, as indicated in Figure 3.1. Thus, a mistaken intervention, such as terminating the operation of an engineered safety feature, might create a new plant condition in which, for example, decay heat is no longer removed from the core. The unsafe intervention can create new conditions that require new actions by operators, possibly on different time scales, than if no action had been taken. In this way, human interventions (both beneficial and detrimental) requires an iterative consideration for creating new plant conditions and making specific PSFs relevant. When unsafe actions change plant conditions, they create the potential for additional PSFs to become relevant in influencing particular error mechanisms, which can generate further unsafe actions.

In the context of operating experience, there are two forms of unsafe actions that interact with plant conditions: unsafe acts of omission, and unsafe acts of commission. The unsafe acts of omission (UAO) are those where people fail to take an action or series of actions that would put the plant in a safer state, or at least prevent its continued deterioration. The unsafe acts of commission (UAC) are those interventions taken by people that make the plant less safe. As previously discussed, in the PRA context, these unsafe actions of omission or commission do not necessarily correspond with human failure events error of omission (EOO) or error of commission (EOC) modeled in a PRA.

Impact on Human Failure Events

The plant conditions set the context for the consequences of the unsafe action in terms of the impact on plant systems. For instance, omitting a step from a procedure can result in failure to start equipment as described above: this would be an EOO in a PRA. However, omitting a step in a procedure that presented cautions that the following step was to be performed only under certain conditions could result in inappropriately performing the next step (an error of commission (EOC)). The distinction between the two errors is almost entirely set by the impact on plant systems, even though the same unsafe action (e.g., omitting a step in a procedure) is involved.

3.3 Example of Framework Application

An event illustrating the value of the framework is the loss of RHR (and RCS inventory) event at Prairie Island Unit 2 on February 20, 1992, which was the subject of an NRC Regional Augmented Inspection Team (AIT) report. Table 3.2, adopted from NUREG/CR-6093 (Barriere et al.), identifies the essential elements of the event. Operators were reducing the RCS inventory to reach midloop conditions (one of the possible operating states during a refueling outage) on the second day after the reactor was shut down. The reactor's level of decay heat was still relatively high (i.e., approximately 6 MW). As is common

Table 3.2 Summary of Loss of RHR Event, Prairie Island Unit 2, February 20, 1992*

Event: Loss of RHR for 21 minutes

Situation	Acts	Defenses	Conditions	Influences
1. Day 2 of outage; decay heat is high (approximately 6 MW). In-vessel boiling occurred. 2. Installed permanent level instrumentation not compatible with planned evolution (N_2 gas overpressure). 3. Temporary level instrumentation required accurate manual calculations. 4. Both permanent and temporary redundant instrumentation relied on single common pressure-measurement sensor. 5. Small errors in estimated timescale for drain to midloop led to unacceptable plant conditions (airbinding of cooling pumps).	1. Two rounding errors made by operators in calculating RCS level. 2. Operators over-reduce RCS level, which causes vortex (this is based on Shift Manager's faulty calculation of drain-down time). RHR pump fails due to airbinding. 3. Little discussion with shift operations management about problems during event.	1. Multiple RCS refill routes available. *+Design* 2. Operators trip RHR pump on early evidence of airbinding. *+Training* 3. Once RHR pump was tripped, AOP and EOP led operators to successful recovery. *+Procedures* 4. Containment evacuated according to procedure. *+Procedures*	1. Two related procedures (RCS level and draindown time) required extensive, detailed calculations with no aids provided. *-Human Engineering* 2. Temporary RCS level instrumentation very difficult to read in poor environment. *-Human Engineering* 3. Operating personnel had limited or no training in draindown tasks. Experienced personnel allocated to other parallel tasks. *-Training, Supervision* 4. Draindown procedure not clear on prerequisites for instrumentation availability. *-Procedures* No communication with shift operations management led to lost opportunities to correct errors in level control. *-Communications* 5. No communications from plant personnel, who heard pump "burping," led to delay in identifying impending airbinding. *-Communications*	Procedures: -1; +2 Training: -1; +1 Communications: -2 Human Engineering: -2 Supervision: -1 Design: +1

Source: AIT Report 50-306/92-005.

---

* + indicates a positive defense, condition, or influence in the event
  - indicates a negative defense, condition, or influence in the event

practice at other reactors, the reactor water level was being measured by a temporary level-measurement system using a tygon tube because the permanently installed electronic instrumentation was not compatible with the plant conditions associated with nitrogen overpressurization. Using this temporary instrumentation required the operators to calculate the water level to take account of the effects of nitrogen overpressurization. In addition, the operators used the calculated draindown rate to estimate the time when the targeted midloop level would be reached. Because of a combination of several calculational errors and poor communication between the operating crew and their supervisors, the RCS level was reduced to the extent that suction pressure to the pump used for core cooling (one RHR pump) was lost. The pump became airbound and core cooling was lost for 21 minutes, and because of the level of the decay heat, boiling in the reactor took place. In addition, the containment was open, with temporary cables passing through open penetrations, and the mechanical interlocks on the personnel access door was disabled.

Using this event, the following observations can be made, referring to the framework. Figure 3.2 illustrates the framework's representation of this event and the relationships between elements. First, the human failure event was overdraining the RCS, causing a loss of RHR; this would constitute a LOCA initiating event in a LP&S PRA. This classification indicates that recovery of core cooling involves more than simply restoring operation of the RHR pump; refilling the RCS and sufficiently venting for the RHR pump to operate is a prerequisite before restoring core cooling, which has an impact in the recovery analysis.

This human failure event resulted from two unsafe actions: a miscalculation of the RCS water level, and of the time to reach the target midloop level (only partly influenced by the first miscalculation). These unsafe actions were the result of error mechanisms associated with situation assessment and response planning which, when combined, reflected the incomplete knowledge of the draindown crew and supervisor. In part, these unsafe actions were influenced by the PSF-supervision, as demonstrated by the lack of communication by operations supervisors who could have detected these errors from their experience during previous similar operations.

Both unsafe actions were "rule-based mistakes". The procedures gave no direct guidance on the accuracy required in the calculations. In addition, important parameters were not provided, and checkpoints were not included in the procedure that could have revealed the incorrect level calculation. These procedures were followed and applied by the operators as written.

The primary PSF for these two mistakes were inadequacies in the procedures. In addition, the operators making the calculations had not been trained in the procedure and had not performed the task before. The lack of supervision allowed the errors to continue. Of somewhat peripheral importance to this event was the difficulty in reading the actual level indicated on the temporary instrumentation, i.e., tygon tube, indicative of an HSI deficiency.

The plant conditions were of considerable importance in this event. First, the high decay-heat level created the hazard whereby the core could be put at risk by a relatively brief loss of cooling. Second, the reactor vessels water level instrumentation was inoperable as a result of the design of its electronics that rendered it offscale by the nitrogen overpressurization condition; hence, the Emergency Response Computer System (ERCS) indicated a "failed" status in the control room. Third, the draindown task was sensitive to small errors in the calculations, such as rounding of results, and discrepancies between sources describing cross-sectional areas of tanks.

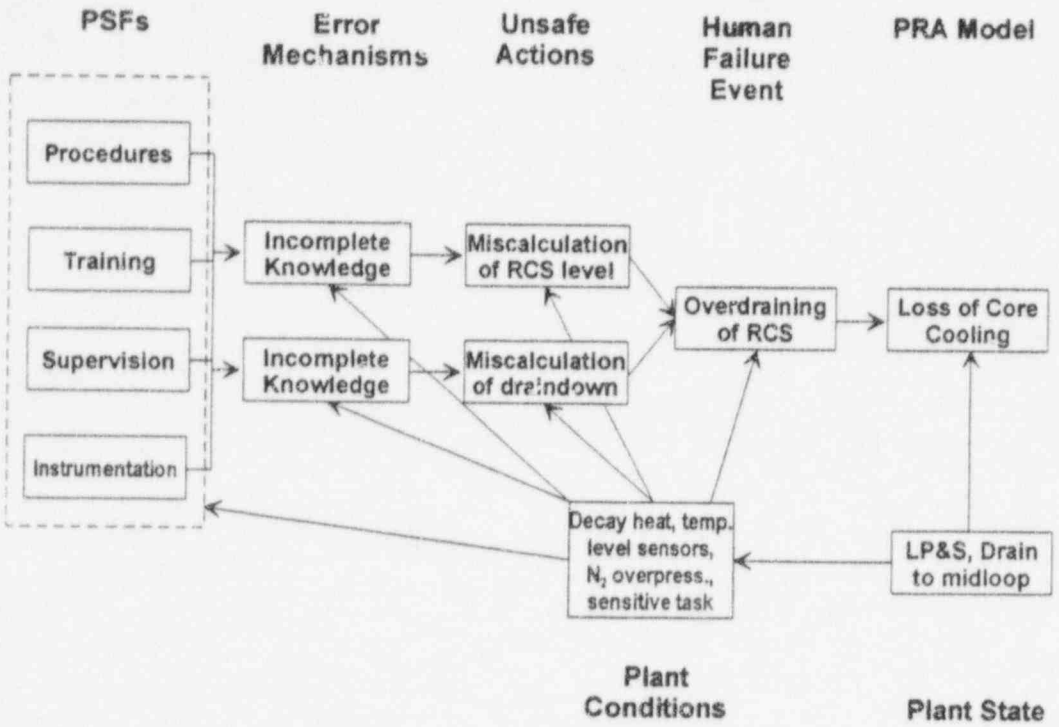


Figure 3.2 Framework representation of February 1992 Prairie Island Unit 2 loss of RHR event

3.4 Framework Conclusions

The multidisciplinary HRA framework provides a structure that explicitly relates, focusses, and encompasses the disciplines of human factors, psychology, human reliability analysis, and probabilistic risk assessment. The framework can be used as a basis for analyzing event reports and deriving data and insights. It can enrich the qualitative analysis of operational events, particularly by focusing on the interactions between human performance and plant conditions that resulted in significant events. Programs aimed at only human performance or plant conditions will never be entirely successful because it is their interplay and synergistic effect that cause significant events.

The interaction between human performance and plant conditions is further exemplified by the characteristics of major accidents discussed in Section 2, i.e., operating outside the designer's intention, thereby entering a regime where plant behavior is not understood, followed by failure to believe accumulating evidence. These characteristics appear to be supported by the framework and events analyzed in its context. This breakdown is currently not reflected in PRAs, and without it, PRA can only partially reflect the causes of risk.

This framework continues to evolve. As knowledge in the behavioral sciences develops, as more events are reviewed, and as subsequent tasks are performed, we anticipated that the framework will expand.

Its capability to be easily adaptable and expandable is seen as an important feature. No finding from actual events should be discarded simply because "it doesn't fit the model" nor should any area relevant to human performance in NPP activities be excluded because "it's not in the scope." On the other hand, elements are included, modified, or refined only when they are potentially important to understanding NPP safety.

4. ERRORS OF COMMISSION

4.1 Introduction

Errors of commission (EOCs) were identified as a critical area for human reliability analysis (HRA) during the Project Assessment Phase based on the review of operational experience during LP&S events (NUREG/CR-6093). Consequently, the project's Analysis and Characterization Phase also considered important EOCs pertaining to at-power operations. The primary objectives concerning EOCs were to develop the understanding necessary to bound the potentially infinite number of human actions which could be called "errors of commission," identify their key features which could form the basis for quantification methods, and develop guidance for identifying and modeling EOCs in support of PRAs.

To accomplish these objectives, three activities were pursued:

(1) characterize potential causes of EOCs and principles for modeling them,

(2) identify opportunities for EOCs, and

(3) develop guidance to HRA and PRA analysts for identifying and representing a focused set of potentially risk-significant EOCs in PRA models.

Appendix B contains the detailed report which documents the specific EOC developments made in the Analysis and Characterization Phase. The key insights and developments from this report are summarized next. Following a discussion on the definition of an EOC in Section 4.2, Section 4.3 describes the approach used for identifying and characterizing EOCs. Section 4.4 discusses the identification of EOC opportunities, while Section 4.5 gives guidance for EOC modeling. Finally, Section 4.6 summarizes EOC conclusions. The results of this work, in conjunction with multidisciplinary HRA framework and human dependency developments, will serve as inputs in the future development of HRA quantification methods.

4.2 EOC Definition

The term "error of commission" has been used variously for several years. The present (Improved HRA) project team specifically defines an EOC as a human failure event that represents:

> *an overt, unsafe action that, when taken, leads to a change in plant configuration with the consequence of a degraded plant state.*

This definition is consistent with the multidisciplinary HRA framework and is based on the review of operational experience, and the objectives of improving HRA and PRA methods. By this definition, the EOCs of interest do not include all random actions that occur in the plant. Rather, one of the important goals of the project is to focus more narrowly upon those EOCs that degrade plant safety and, therefore, should be included within the scope of PRA.

In particular, the multidisciplinary HRA framework recognizes "error of commission" as a PRA term describing the potential manifestations of a human failure event on the hardware portion of the PRA model. By recognizing "error of commission" in the context of the PRA model (or, more broadly, safety and risk-significance), the myriad human actions that could potentially be labelled "errors of commission"

can be effectively bounded; only those actions which impact plant safety functions, safety systems, and other risk-relevant equipment should be modeled in the PRA. Furthermore, the specific modeling of EOCs depends upon what the PRA is modeling (e.g., LP&S and at-power operations), its objectives (e.g., understanding of risk vulnerabilities, risk management, design verification), and the state-of-the-art in HRA and PRA. Hence, an EOC represents a human-failure event in a PRA that is identified and defined from the knowledge and understanding of plant conditions, PSFs and error mechanisms, and their associated unsafe human actions.

4.3 Approach for Identifying and Characterizing EOCs

The results of event data analyses are used for identifying and characterizing EOCs. Based upon our analyses, the most information-rich sources are the detailed event descriptions given in AEOD Human Performance Studies and Regional Augmented Inspection Team reports, followed by full-text Licensee Event Reports (LERs). The results presented in this subsection are based upon these information-rich data sources.

As identified in Section 3, there is a distinction between human failure events and unsafe actions which is relevant to using historical event data in characterizing EOCs. The definition of human failure events depends upon the context of the PRA model (e.g., plant states, initiating event type). Consequently, historical event data cannot be used to define EOCs, or even errors of omission (EOOs), without a specific PRA context. However, historical event data can identify unsafe acts of commission (UACs) and unsafe acts of omission (UAOs). The relationship established by the multidisciplinary HRA framework between UACs and EOCs (which should be represented as human failure events in the PRA) gives insights on the causes of EOCs, influences on EOCs, and characteristics of EOCs in general from investigations of UACs in event data. The analysis strategy taken for this task takes advantage of this relationship between UACs in historical event data and EOCs expected to be modeled in PRAs.

EOC analyses based upon full-text LERs and event-based reports are given separately in the following subsections. Since the LERs are more numerous, some statistics were investigated in the analysis and are discussed in NUREG/CR-6093. On the other hand, the event-based reports contain more detailed information for drawing qualitative insights but are, in themselves, insufficient for statistical analyses.

4.3.1 EOC Insights from Full-Test LER Data

The Human Action Classification Scheme (HACS) database of analyzed PWR LP&S events, developed in earlier work and reported in NUREG/CR-6093 (Barriere et al., 1994), contains 39 unsafe acts and associated information on human performance. Although these results are specific to LP&S conditions, some have implications for other conditions and, therefore, represent significant insights for performing future PRAs. Examples of such important insights are:

- UACs occur more frequently than UAOs in LP&S,
- human-induced initiators, especially UACs, are the most frequently occurring error kind during LP&S,
- mistakes are the predominant error type for UACs,
- "procedures" is the most frequently cited negative PSF associated with UACs, followed by human-system interface (HSI) and training, and
- for UAC initiators, "procedures" is the most frequently cited negative PSF associated with both slips and mistakes.

4.3.2 EOC Insights from Detailed Report-Based Events

The analyzed results from the following five events discussed in NRC/AEOD Human Performance Study reports and/or NRC Regional AIT reports were judged to be useful for further investigation and characterization of the causes of EOCs: Braidwood Unit 1 (12/1/89), Loss of RCS Inventory (transition from cold to hot shutdown); Braidwood Unit 1 (10/4/90), Loss of RCS Inventory (during LP&S); Crystal River Unit 3 (12/8/91), Loss of RCS Pressure Transient (startup); Oconee Unit 3 (3/8/91), Loss of RCS Inventory (during LP&S); and Prairie Island Unit 2 (2/20/92), Loss of RHR (draining to midloop). With one exception, all of the unsafe acts identified in these events are UACs. In addition, all identified unsafe acts are mistakes. To utilize all available information on post-accident responses, intermediate actions (which would have been unsafe acts if uncorrected) were included in this analysis. All of the intermediate (or sub-optimal) actions in the reports of the five events also are classified as UAC mistakes.

Our preliminary results suggest that the underlying causes of EOCs differ for unsafe acts in the pre-accident or initiating event phase compared to those which occur in response to accidents. Consequently, pre-accident and initiating actions are discussed separately from post-accident actions. Appendix B gives a complete discussion of the detailed report-based event analyses.

Insights Regarding Pre-Accident and Initiator Unsafe Acts

Three of the five event-based reports contained significant pre-accident and/or initiator UACs: Braidwood Unit 1 (10/4/90), Prairie Island Unit 2 (2/20/92), and Oconee Unit 3 (3/8/91). All three events occurred during LP&S operations. The most important influences on the unsafe acts seem to be performance shaping factors (PSFs) and significant or unusual plant conditions at the time of the event. Table 4.1 summarizes the important PSFs (by category only) and significant or unusual plant conditions for each event and unsafe act. (The number of any multiple effects for the same PSF category identified are shown in parentheses.) Table 4.1 illustrates several important points about PSFs:

- multiple PSFs were involved in all three events,
- all of the PSFs identified are negative influences (e.g., no significant positive aids to task performance were identified), and
- procedures were important to all three events.

Furthermore, there were several common PSFs in the unsafe acts in all three events. For example, in the Braidwood Unit 1 (10/4/90) event, the pre-accident and initiating events were coupled temporally (e.g., actions involved were part of the same process and occurred close together in time), by common personnel, and by common PSFs. The specific negative effects from these common PSFs were: 1) Procedures - no procedural guidance for performing two surveillance tests together (the activity in progress), 2) Stress - the two key personnel involved had worked 19 and 17 hours, respectively (e.g., overtime), 3) Communications - the shift turnover briefing which took place before the unsafe acts did not state that two tests were being performed simultaneously, 4) Communications - the engineer in charge of the two tests did not wait for verbal confirmation that the RHR vent valve was closed, and 5) Organizational Factors - normal command, control, and communications were not in force since the control room crew (e.g., shift engineer, shift control room engineer, and board operators) was not aware of the planned changes to the RCS configuration.

Table 4.1 Characteristics of Pre-Accident and Initiator Unsafe Acts

Event Identifier/Significant or Unusual Plant Conditions	Action*	PSFs**
Braidwood 1: (10/4/90) (Loss of RCS Inventory) • Planned breach of RCS pressure boundary • Two procedures performed simultaneously	P: Did not wait for confirmation that RHR vent valve was closed	- Procedures - Stress - Communications (3) - Organizational factors
	I: Drain-path created by opening RHR hot leg suction valve	- Procedures - Stress - Communications (2) - Organizational factors
Prairie Island 2: (2/20/92) (Loss of RHR) • Planned RCS draindown • N_2 pressure higher than normal • Inexperienced draindown crew	P: Errors in RV level determination	- Human-System interface - Procedures (2) - Supervision - Training - Communication - Instrumentation
	P: Inadequate N_2 pressure control	- Procedures - Training
	I: Overdraining of RCS	- Human-System interface - Procedures (2) - Supervision - Training - Communication - Instrumentation
Oconee 3: (3/8/91) (Loss of RCS Inventory) • Planned breach of RCS pressure boundary	P: Blind flange on wrong LPI sump line	- Human-System interface - Procedures - Training (2) - Organizational factors (2)
	P: Independent checking failed	- Human-System interface - Procedures - Training - Organizational factors
	I: RCS drain-path through unblanked line	- Organizational factors - Procedures - Communications

*P = Pre-accident unsafe act, I = Initiating unsafe act

** (#) = number of multiple effects for same PSF category

In these three events, the procedural deficiencies involved either a lack of completeness (e.g., situation not covered) or no procedure. This type of procedural deficiency under-specified how tasks were to be performed, representing a gap in guidance allowing undesired variability in performance of the task. Because all three events involved multiple PSFs, the lack of procedural guidance may also have created the opportunity for additional negative PSFs to have a significant influence on task performance.

All three events shown in Table 4.1, represent planned activities which did not go as planned, and involved a significant unusual change in plant conditions. Also, all three events involved sensitive operations related to changes in the RCS [e.g., breach of RCS pressure boundary or reduction in reactor vessel (RV) level]. The Oconee Unit 3 event was "set up" by the pre-accident unsafe acts (i.e., a cascading-type dependency) with actions involved in the event initiator representing triggers leading to the discovery of the pre-accident unsafe acts. For both the Braidwood Unit 1 and Prairie Island Unit 2 events, additional unusual circumstances were prevailing before the initiating event which contributed to the occurrence of both pre-accident and initiator unsafe acts. Further, the initiating event in both events resulted from the continuation of activities in progress earlier. In the Braidwood Unit 1 event, two surveillance test procedures were being performed simultaneously for the first time. The lack of procedural and administrative guidance and prior experience in performing the tests together were significant contributors to its occurrence. The Prairie Island Unit 2 event also involved previously unencountered conditions. The N_2 pressure was higher than normal, requiring calculations of RV level to involving extrapolations based on lower N_2 pressures. In addition, on previous occasions experienced crews had performed RCS draindowns (including the assistance of an experienced systems engineer). On that occasion, both the draindown operators and the assisting systems engineer were inexperienced.

Insights Regarding Post-Accidents Unsafe Actions

All five event-based reports were useful in investigating and characterizing causes of post-accident EOCs through the identification and analysis of UACs. Both post-accident actions and intermediate, sub-optimal actions are discussed in this section.

The two Braidwood Unit 1 events, and those at Prairie Island Unit 2, Oconee Unit 3, and Crystal River Unit 3, suggest that PSFs and cues for diagnosis are the important influences on the opportunities for post-accident UACs. Although both the Braidwood Unit 1 (10/4/90) and Prairie Island Unit 2 events involved significant and unusual conditions, these conditions no longer existed at the time of accident response (Table 4.1).

Table 4.2 illustrates three points about the influence of PSFs on accident response. First, like pre-accident and initiating unsafe acts, multiple PSFs are active for many of the actions shown in Table 4.2. Second, most of the PSFs which play a role in post-accident actions are positive factors in task performance. In fact, only positive PSFs were identified for the successful post-accident actions while the intermediate, sub-optimal actions had only one or two negative PSFs in addition to positive PSFs. Third, comparison of Tables 4.1 and 4.2 reveals that instrumentation is more important in post-accident actions than in pre-accident and initiator unsafe actions: this is consistent with the importance of diagnosis and cues for diagnosis for post-accident actions.

Diagnostic cues primarily consist of control room instrumentation and reports from the plant (e.g., local indications reported by phone). Both the availability and the interpretation of these cues influence the ability to correctly diagnose accident conditions (and confirm successful post-accident actions). Hence, the three categories of diagnosis cues were developed to account for: 1) misleading cues (e.g., failed or

Table 4.2 Characteristics of Post-Accident Actions

Event/Significant Conditions	Action*	PSFs**	Cues for Diagnosis		
			Misleading	Discounted	Used & Useful
Braidwood 1: (10/4/90) (Loss of RCS Inventory) Planned breach of RCS pressure boundary.	P: RCS drainpath isolated	+ Communications			• Phone call to CR re: RCS breach
Prairie Island 2: (2/20/92) (Loss of RHR) Planned breach in RCS pressure boundary.	P: Refill RCS & restore SDC	+ Procedures + Supervision + Instrumentation			• Electronic level indication (came on scale) • RHR pump low flow, low suction pressure & low motor-amp current alarms
Oconee 3: (3/8/91) (Loss of RCS Inventory) Planned breach in RCS pressure boundary.	Sub: Opened BWST suction isolation valves before isolating drainpath to sump	- Instrumentation + Procedure + Communications + Instrumentation	• Reactor building normal sump high-level alarm • RV level decreasing	• Reactor building emergency sump high-level alarm	• RV ultrasonic level alarm • Report from containment re: decreasing RV level & increasing radiation • LPI pump A current fluctuating downward
	P: Isolate drainpath (& closed BWST isolation valves) & refill RCS	+ Instrumentation			• RV level indication
Crystal River 3: (12/8/91) (Loss of RCS Pressure Transient) Startup/transition in power.	Sub: Increased RX power before knowing reason for RCS pressure decrease Sub: Bypassed ESFAS before knowing reason for RCS pressure decrease	+ Instrumentation - Instrumentation - Procedures	• PZR spray valve indication (shows closed even though valve is open) • Report re: steam flow to deaerating feed tank	• PZR level increasing • RCS temperature decreasing	• RCS pressure decreasing • RV level, sump levels, radiation monitors (i.e., no LOCA) • S/F & feedrates normal
	P: Close PZR spray valve & control RCS pressure	+ Instrumentation - Procedures and/or training			• RCS pressure trends • PZR vapor space temperature trends
Braidwood 1: (12/1/89) (Loss of RCS Inventory) Preparing to enter hot shutdown from cold shutdown (i.e., drawing PZR bubble & increasing RCS pressure)	Sub: Isolated operating RHR B train	+ Instrumentation + Communications - Procedures + Training - Training	• Report of leak in vicinity of RHR A relief valve		• Containment parameters (pressure, humidity, temperature, sump levels) (i.e., not in containment) • PZR level, RHR pump motor current • Reports on holdup tank level increase • RCS pressure decreasing
	P: Isolated RHR A train (w/ open RV) & restored PZR level	+ Training + Communications + Instrumentation			• Report of flow through RHR B relief valve • PZR level & RCS pressure trends

*P = Successful post-accident action; Sub = Sub-optimal, intermediate action

** - indicates a positive PSF effect
+ indicates a negative PSF effect

flawed instrumentation) or misinterpreted information, 2) accurate information that is rejected, and 3) helpful information that leads to successful accident response.

Table 4.2 illustrates two different kinds of events and their diagnosis: 1) for two events, only successful post-accident actions were identified and 2) for the other three events, sub-optimal actions, as well as successful post-accident actions, were identified. Immediate, successful post-accident actions were achieved in both the Braidwood Unit 1 (10/4/90) and Prairie Island Unit 2 events. No intermediate, sub-optimal actions were identified. Also, all of the PSFs were positive and all of the accident cues were unambiguous and were acted upon (e.g., only "used & useful" cues).

Sub-optimal actions and negative PSFs, including misleading cues, were identified in the Oconee Unit 3, Crystal River Unit 3, and Braidwood Unit 1 (12/1/89) events. In addition, useful information was rejected or discounted in the initial response to the Oconee Unit 3 and Crystal River Unit 3 events. Reviews of the event timelines and operator interviews given in all three reports revealed that an initial, erroneous mindset had to be overcome before achieving a successful accident response. Furthermore, misleading cues were used to support the initial erroneous mindset in all three events, while useful information which was inconsistent with the mindset was initially discounted in the Oconee Unit 3 and Crystal River Unit 3 events. The successful response to the accident in all cases appears to have resulted from an "initial mindset breaker", either a single unrefutable cue or the accumulation of information.

In the Oconee Unit 3 event, both the high level alarm for the reactor building containment sump and the decreasing RV level indication were discounted. According to the timeline, operators conjectured that the RV level transmitter was malfunctioning. In addition, the sump high level alarm was attributed to washdown operations which occurred earlier in the outage. From these interpretations, it is surmised that operators did not initially recognize the existence of an RCS drain-path. Reports from the reactor building about the decreasing RV level and increasing radiation appeared to be the convincing factors that an RCS drain-path existed. Awareness of the testing on the RHR sump isolation valve and the indication that RCS level was not increasing, even with injection from the Borated Storage Water Tank (BWST), eventually led operators to close both RHR sump isolation valves, terminating the draining of the RCS. Indication of increasing RV levels, after isolating the sump valves, confirmed the success of the final post-accident actions.

4.3.3 Implications of Insights Regarding EOCs

Several important implications can be drawn from the results of this data analysis. The implications of the LER and report-based event analyses are discussed separately below.

The PWR LP&S implications of the LER results is that PRAs which address all modes of plant operation should include EOCs, especially human-induced initiators and mistakes, due to their frequent occurrence in LP&S operational experience. Also, improved HRA quantification methods must continue to address the influence of procedures on human performance. The influences of HSI and training also should be addressed. In addition, the implication of the importance of procedures to both slips and mistakes is that improvements in procedures must encompass both format and content, since slips are commonly associated with formatting, and mistakes with technical deficiencies in procedures.

From the reviews of report-based events, two important insights can be drawn from the analyses of pre-accident and initiator unsafe acts. First, the consistency of results with respect to PSFs between all five events (as well as the LER results) implies that, under current plant practices and the present regulatory

environment, it is reasonable to expect that multiple, negative PSFs are likely to influence most plant activities. Consequently, the "stage" is already set and, given the opportunity, an EOC is likely to be committed. Second, the opportunities for EOCs, which are discussed further in the next section, should be defined by the activities which involve plant interventions, and the associated conditions under which they are performed.

Using the insights from the analysis of report-based event descriptions, the role of diagnostic cues in confirming an initial erroneous mindset, and in breaking it, can be compared to the concept of confirmation bias (Reason, 1990). In all three cases in which sub-optimal recoveries occurred, a mindset, which seemed to be derived from past experience or training, prevailed as the initial diagnosis of the event. In some cases, early indications matched this initial mindset, confirming the erroneous diagnosis. The break from the initial mindset was achieved only after there was completely unambiguous and/or cumulative evidence to the contrary.

As discussed in Section 2, there have been common factors in the most notable events which have occurred in nuclear power history (e.g., Chernobyl, TMI-2) which are also common to the events (particularly LP&S) analyzed for this project:

(1) the plant is operated outside the designer's intentions,
(2) the plant then enters a regime where its behavior was not clearly understood, and
(3) operators refuse to believe accumulating evidence.

These elements are noticeable in the events shown in Tables 4.1 and 4.2. For example, insufficient guidance in procedures for many of these events led to non-proceduralized actions which deviated from good operating practices (especially, Braidwood 1 (10/4/90) in which two procedures were performed simultaneously). Also, insufficient understanding of the plant behavior is evident in the Prairie Island Unit 2 event (e.g., misunderstanding about implication of high N_2 pressure) and in the Crystal River Unit 3 event (e.g., lack of understanding as the cause of the RCS pressure transient). In other events, there seemed to be a lack of sensitivity to the importance of changes in RCS configuration (e.g., planned breaches in RCS pressure boundaries in Braidwood Unit 1 and Oconee Unit 3 events). The two of the three events which involved sub-optimal recoveries (Table 4.2), illustrate situations in which operators refused to believe instrumentation which was, in fact, providing reliable information.

4.4 Identification of Opportunities for EOCs

An approach for identifying EOC opportunities was developed to extend the insights derived from our reviews of operational experience. In particular, two different approaches are recommended for different time phases.

As previously described, for pre-accident and initiator unsafe actions (especially during LP&S), the "stage is already set," due to the likely existence of negative PSFs, for EOCs to be committed and the only additional factor needed is the opportunity. In other words, investigating the features of PSFs which would be in effect when an EOC is committed most likely would not give useful insights on the occurrence of EOCs. It is reasonable to infer from operational experience that current plant operations will include multiple, negative influences, i.e., PSFs, on human performance. The opportunities for EOCs, however, are more a function of a plant's design, conditions, and activities. Consequently, they represent a more efficient, focused approach for identifying potential pre-accident and initiator EOCs.

The previous section described both the cues for diagnosis and the existence of an initial mindset as important in EOC occurrence in the post-accident time phase. Control room instrumentation is the most frequently used, although not the only, source of information used to prompt operators to perform appropriate accident responses. Operator training and procedures comprise the likely sources of initial mindsets. In addition, procedures usually will refer to instrumentation to be used in responding to an accident. Therefore, for the post-accident time phase, analysis of procedures and training PSFs, as well as instrumentation availability, could lead to important insights about post-accident EOCs.

Based upon the above discussion, two approaches to EOC opportunity searches are recommended:

(1) **Mechanism Search** - For pre-accident or initiator unsafe acts, a defense-oriented search approach should be conducted based upon plant design and configuration, coupled with an investigation of controls, or limits, on plant conditions (especially unusual or previously unencountered conditions) and potential plant activities.

(2) **Procedure Search** - For post-accident unsafe acts and some initiators, a procedure search approach should be conducted that includes considering uncertainty at decision points requiring various PSFs (such as instrumentation that may be applicable in accident diagnosis). Its focus would be on emergency operating procedures (EOPs) for post-accident unsafe acts and outage process procedures for LP&S initiators, and should include the identification of necessary instrumentation/information requirements and potential limitations.

Thus far, the feasibility of these two approaches has been explored but not definitively demonstrated; they will be further refined in the next phase of the project.

4.5 Guidance for Modeling EOCs

From the event analyses described above, a candidate set of rules for identifying a limited scope of risk-significant EOCs to be included in PRA models was devised that is compatible with, and builds upon, current HRA modeling practices. The following a brief summary of the general guidelines suggested for modeling EOCs which is elaborated on in Appendix B.

(1) Different HRA/PRA modeling (i.e., identification, representation, and quantification) techniques are required for EOCs included in PRAs for different plant operating modes (e.g., full-power, startup, shutdown) and different types of events (e.g., loss of electric power, loss of RHR).

(2) To identify the reasons or opportunities for plant intervention and, therefore, opportunities for EOCs, examine plant conditions which are characteristic of each operating mode modeled.

(3) Investigate task - (or intervention-) specific PSFs, plant conditions, and instrumentation issues as possible "triggers" for inappropriate interventions with the plant.

(4) Give special attention to dependent unsafe acts; in particular, all classes of unsafe acts which are typically modeled (e.g., pre-accident, post-accident) should still be modeled as usual, supplemented by those initiating and pre-accident events which depend on other events.

Appendix B also discusses our preliminary insights that will be used to develop further guidance specific to different plant operating modes and events.

4.6 EOC Conclusions

The research efforts summarized in this section provide valuable insights on EOCs which further our understanding of human performance, in general, and pave the way for developing improved methods for HRA modeling, quantification, and associated guidance.

UACs occur in both LP&S and at-power events. These UACs are not acts of sabotage. Rather, they are unsafe acts consistent with the traditional HRA definitions of events which should be modeled in PRAs. These UACs are risk-significant actions which are involved in the development of accident sequences. Consequently, such UACs deserve consideration for explicit modeling in PRAs as EOCs.

This work indicates that EOCs can be bounded. Certain EOCs can continue to be modeled implicitly in PRAs through initiating event frequencies and hardware unavailabilities. The EOCs which should be explicitly modeled in PRAs, can be found through the approaches for identifying opportunities for them. Section 7 discusses further implications of these insights. The next phase of this project will refine the guidance on which EOCs to explicitly or implicitly model, and also appropriate search techniques to use; e.g., procedures (EOPs) and mechanism searches.

The underlying influences of EOCs; e.g., PSFs and plant conditions, can be characterized with the multidisciplinary HRA framework. This work included an investigation of a familiar set of influences on the UACs identified in PWR LP&S LERs and event-based reports. However, identifying important EOC characteristics required a break from the familiar perspective on human reliability influences and the underlying assumptions of PRA models. For instance; plant conditions, defined in more detail than currently used in PRA models, were shown to be important influences on both human performance and accident consequences in LP&S events. For at-power events, the specific physical plant conditions for certain classes of actual events which involve EOCs (e.g., transient, small break LOCAs) may not be recognized or well understood. Consequently, these conditions may not be explicitly considered by either plant procedures and training or by the PRA model. Furthermore, instrumentation cannot always be assumed to be available and reliable (especially during LP&S conditions and during changes in plant state). Interpretation of instrument indications and implementation of procedures cannot be assumed to be correct or uniform under the variety of possible plant conditions. Thus; plant conditions, PSFs, and instrumentation are important factors identifying, representing, and quantifying EOCs, due to their significant influence on EOC occurrence.

In summary, rationality and order can be brought to modeling EOCs. The work completed so far, and that planned, will be a stepwise improvement in current PRA modeling practices, rather than a complete departure from them. These insights will be incorporated into an improved, integrated HRA/PRA approach during the next phase of the project.

5. HUMAN DEPENDENCY

5.1 Introduction

The term "human dependency" describes the situation where the outcome of a particular human action is related to, and influenced by, the outcome of an earlier action or actions (i.e., the outcome of the subsequent action is not independent of preceding actions). For example, in a 1991 LP&S event at Oconee Unit 3, a blind flange was installed in the wrong penetration line from the containment sump to an RHR pump (a pre-accident unsafe action). Subsequently, operators "stroke-tested" a valve in the line that should have been blocked but which, in fact, was open to the sump. As a result, almost 10,000 gallons of reactor coolant was drained to the sump from the RCS. The incorrect installation of the blind flange and the subsequent failure to confirm that the line with the valve being tested was blocked were not independent; both unsafe actions resulted from all the operators relying on an incorrect and unauthorized label used to identify the line. This event is discussed further in Section 5.4.

In PRA terms, it is recognized that dependency has the property of two or more PRA human failure events (a, b); e.g., involving unsafe actions in the pre-accident, initiator and/or post-accident phase, that causes the following probabilistic relationship to be true:

$$P(a,b) \neq P(a) \times P(b)$$

As discussed in Section 5.3, several different kinds of dependence mechanisms can cause this relationship. In most cases, the dependence mechanisms of concern are those that influence multiple human actions in the same PRA cut-set. In keeping with the development of the framework, a multidisciplinary approach was taken to identify and characterize the dependence mechanisms, including the perspectives of plant engineering, PRA, and the behavioral sciences.

5.2 Framework for Identification of Dependence Causal Mechanisms

Section 3 described the multidisciplinary HRA framework that identifies how unsafe actions can impact safety and their relationships with the logic models used in PRAs. The framework is divided into several elements including PSFs, error mechanisms, unsafe actions, plant conditions, and human failure events. PSFs and plant conditions play a critical role in the occurrence and form of error mechanisms whose consequences are observed as unsafe actions. Consequently, both influence the occurrence and consequence of unsafe actions. Furthermore, unsafe actions can change plant conditions and make additional PSFs more relevant in creating the opportunity for subsequent; i.e., dependent, unsafe actions.

In addition to their unique contribution to dependence between unsafe actions, PSFs and plant conditions potentially can originate in common (organizational) processes. For example, ineffective procedure development or training programs could lead to deficiencies in those PSFs for a variety of plant personnel involved in numerous activities. Similarly, poor planning could allow multiple activities to be performed simultaneously, which can create an unanalyzed plant condition. Catalogs of organizational processes have been developed in research programs associated with organizational processes and their influence on safety, such as those performed by BNL (Haber et al., 1991), University of California at Los Angeles (Davoudian et al., 1994), and Science Applications International Corporation (Wreathall et al., 1990).

5.3 Types of Dependence Causal Mechanisms

Appendix C discusses two failure paths by which dependence mechanisms can influence unsafe actions i.e., latent and active human failures. Latent human failures are typically pre-accident unsafe actions that remain hidden, possibly for some considerable time. An example was the installation of the blind flange in the wrong line in the 1991 Oconee Unit 3 event. While that unsafe action did not cause any immediate safety problem, it removed an important safety defense against inadvertent RCS draining. Alternatively, active human failures are typically initiator or post-accident unsafe actions whose consequences are revealed immediately, due to their direct impact on plant systems. The active UAC associated with valve stroke-testing in the Oconee event, without correctly verifying that the line to be tested was, in fact, blocked, had the immediate effect of releasing RCS inventory to the containment sump. Many UACs associated with initiating events are active human failures that should be represented as EOCs in PRA human-failure events.

Dependence mechanisms associated with a combination of latent and active human failures are particularly important in PRAs because they can both initiate an accident sequence, and cause failures of the installed barriers and defenses. This can change the relative contribution to risk of such sequences, as well as dramatically increase the frequency of core damage, compared with sequences where such failures are truly independent.

Active and latent failure paths may originate from (e.g., be dependent on) a set of *common processes*, comprising the activities within the organization, such as planning, procedure development and scheduling, that fundamentally influence all plant-wide activities important to safety. They can be considered specific common-cause mechanisms. For example, during an outage, such a common process could lead to the scheduling of maintenance on a component without ensuring alternative equipment is available (a latent failure potentially involving a loss of a defense). Thus, when replacing RCS level instruments during draindown of the RCS level to midloop, the probability of an active operator error is greatly increased, leading to an inadvertent excessive draindown and loss of RHR.

However, not all dependencies result directly from common processes; instead, *common PSFs* may influence the probabilities of occurrence for multiple unsafe acts. Simple examples include the workplace environment (e.g., heat, light, displays), procedures and training, and factors directly related to human behavior, such as morale and local peer work-norms.

In addition to common processes and common PSFs, *plant conditions* could result in levels of dependence between multiple unsafe acts; these include timing between events (e.g., one event masks or coincides with another), the rates of change in the plant's parameters, and the inherent hazards associated with unique plant evolutions. For example, the potential hazards associated with draining of the RCS to midloop during cold shutdown are much greater shortly after reactor shutdown (when the decay heat is high) than after an extended time. Hence, unsafe actions that normally would be considered independent, because there is adequate time for operators to diagnose and correct each of them, now compete with each other in terms of the resources to diagnose and correct them. For instance, during the 1992 Prairie Island Unit 2 event where RCS overdraining occurred within 48 hours of the shutdown, operators only had a time window of about 20 minutes to diagnose and correct all failures associated with loss of RHR (NRC/AEOD Human Performance Study).

Finally, there can be cases where *one failure causes another*, particularly when one failure changes the plant's conditions in subtle or hidden ways. For example, a latent failure could occur when calibrating

level measurements; the miscalibrated instrument subsequently could lead an operator to over-drain the reactor vessel (RV). The miscalibration can change the plant conditions and influence the consequence of subsequent human actions. This potential is not discussed as a primary causal mechanism because of the initial influences of a common process, common PSFs, or initial plant conditions (or, indeed, a combination of all three).

5.4 Review of Causes of Dependent Events

In this section, experience is reviewed on the causes of dependent events, as defined above. Each of the three categories of dependence causal mechanisms will be evaluated. To help in this evaluation, examples of these casual mechanisms are quoted from one of the significant operational events described previously, the 1991 event at Oconee Unit 3 (NRC/AEOD Human Performance Study and NRC Regional Augmented Inspection Team Report). Table 5.1 summarizes the event in terms of the multidisciplinary HRA framework and the related dependence mechanisms.

5.4.1 Common Processes

Common processes are those that, by their nature, are common-mode influences to whole groups of human actions, such as; management decisions, work organization and planning, procedure and training development, and other programmatic functions within the plant or utility. Deficiencies in these processes can lead to poor or erroneous performance simultaneously in most departments, and between work teams within departments. One simple example would be the case where a lack of work planning led to the simultaneous maintenance of two redundant trains of diesel generators during a refueling outage. A second would be the development of technically inaccurate procedures within the procedure-writing function, leading to errors in performance by both operations and maintenance.

Table 5.1 shows the existence of common processes as influences in the Oconee event. First, there were common deficiencies in the written instructions (procedures and work orders) about the formal identification of equipment. Neither the work instructions, nor the procedures used to check the work formally identified the specific penetration number, so that two groups of operators separately used informal markings for identification. A further procedural deficiency was the absence of any requirement for the final group of operators to confirm or recheck that the blind flange was correctly installed before opening an un-isolated RCS drain path. This combination of deficiencies is an initial indication that the procedure development program at that plant, at that time, was deficient.

In addition, the lack of any true independent checking by the second group of operators and by the operators immediately before opening the isolation valves indicated a common over-reliance on the work performed previously. There seemed to be no analysis of how the penetration could have not been isolated by the blind flange, and therefore, what steps were required to confirm the correctness of the installation, either by the operator "checker" or the test crew. These unsafe actions were well separated in time (several days from start to finish). Rather than being associated with specific PSFs or the local factors such as common supervision, these actions indicate a common organizational process that tolerated the use of informal markings and an over-reliance on the quality of previous work.

Table 5.1 Summary Analysis of Event at Oconee, Unit 3, March 8, 1991

Plant Conditions:		
- Day 24 after refueling		
- No measurements of RCS vessel or loop temperature		
- Containment closed but rad monitors inoperative		
Unsafe Actions:	**PSFs:**	
	Unsafe Action(s)	PSF
1. Blind flange for RHR suction line installed on wrong line - EOC, latent, RB mistake (instructions, label)	(1)	Incorrect use of drawings
	(1)	Procedure did not identify penetration ID #
2. Subsequent checking failed to detect error - EOO, latent, RB mistake (label)	(1,2)	Incorrect informal label
	(1,2)	Poor visibility of formal label
3. RCS drained by operators through unblanked line - EOC, active, KB mistake (no final check by ops, failure to control plant configuration by LO, pursued wrong causes by NLO action)	(3)	Poor communications between maintenance and control room
	(3)	Procedure did not specify coordination between maintenance and operations
	(3)	Lack of task awareness by operations
Dependencies:		
Unsafe Actions	Dependence Mechanisms	
(1-2)	**Common PSFs** - labeling, visibility, organizational processes: control of workspace	
(2-3)	**Common PSFs** - training: unquestioning reliance on prior procedural actions, no double checks (Note: latent failure in (2) set up (3) - temporal)	
(2-3)	**Common (Organizational) Processes** - unquestioning reliance on quality of prior work	
(1,2-3)	**Common (Organizational) Processes** - deficient instructions/procedures: penetration identification # not defined (1) & no requirements for recheck (3)	

In improving HRA methodology, the final quantification process should address the sensitivity to these issues found in the operating experience reviews. Three approaches were developed to evaluate the effects of common processes (Barriere et al., 1994a; Davoudian et al., 1994; Williams, 1991). The potential integration with, and application of, these approaches in formulating an improved HRA methodology will be considered in the current Development Phase of the project. The approaches are briefly summarized below.

The first approach, developed at BNL (Barriere et al., 1994a) is a systematic approach for evaluating quantitatively the influence of organizational factors on estimates of human error probability (HEP). This is accomplished primarily by incorporating organizational factors, in general, into upper and lower HEP uncertainty bounds which establish a "bandwidth" in which revised HEP estimates are calculated, using plant-specific organizational factors. This approach could be expanded to assess the effects of a number of PSFs on HEP estimates, such as human-system interface, procedures, and training.

The second approach, developed at UCLA (Davoudian et al., 1994), involves work-process analyses which evaluate how common organizational processes influence specific task-related PSFs. Methods following this approach face difficulties in considering large numbers (i.e., 20) of organizational dimensions (e.g., common processes) interacting with a comparable number of task factors. Assessing the resulting large numbers of combinations leads to difficulties in the ranking and weighting process since almost all organization dimensions potentially interact with almost all local task factors. Simplifications are being considered to reduce the numbers of ratings, for example, by reviewing the operating-event data for evidence of the more important combinations. It is expected that fewer factors (both organizational and local) would be sufficient to describe most events.

The third approach is that used in the chemical process industries to assess the influence of organizational factors on safety. Several approaches are in use; most are not available to the general public. One such example is the MANAGER assessment system (Williams, 1991), an auditing-based method, in which questionnaires are used to evaluate what are effectively performance indicators associated with specific plant departments, such as operations and maintenance. Indices associated with the "quality" of these departments then are developed to provide a score relative to industry norms. Then, depending on that relative ranking, the numerical results of the PRA are modified based on assumed distributions of the effects of plant norms. In other words, where a plant is rated "10 times better" than the average, the assessed level of risk is adjusted accordingly. This and other similar methods are in constant states of revision, building on improved data. For example, data estimating the effects of management on the failure rates of equipment were reported recently, using data gathered under sponsorship of the U.K. Health & Safety Executive (Wright et al., 1993).

5.4.2 Common Performance Shaping Factors (PSFs)

The category of common PSFs relates to the potential effects of such influences as a common procedure, a common human-systems interface, and a common training program. These influences have the potential, if they are less than adequate, of significantly increasing the probabilities of failures for all those actions that they affect.

An example of such a common influence was during the 1991 Oconee Unit 3 event (Table 5.1). The sequence of errors that occurred were largely (though not exclusively) the result of the operators separately being misled by an erroneous label (e.g., a common PSF), that was not the formal plant label

(which was very difficult to see), but nonetheless misled both the operators installing the blind flange and different operators later checking the installation.

The second example of a common PSF was the deficiency in training, reflected by inadequate checking of prior work. Standard operating practices, such as rechecking the configuration before opening a potential RCS drain path, are normally part of the related training program. However, in this event, the operators opening the isolation valve did not recheck. This failure, together with their failure to detect the incorrect installation, reflects a lack of effective training in standard operating practices.

5.4.3 Plant Conditions

In addition to the common processes and the common PSFs, the plant conditions are important in creating the potential for dependent failures because they create the environment within which all tasks are performed, and therefore significantly influence them. Perhaps the broadest view of the influence of plant conditions influence is during LP&S operations, when many systems and features taken for granted during at-power operations are not available. For instance, the plant may have only one incoming electrical supply and normal instrumentation may be disconnected or non-operational, with operators having to rely on temporary measuring systems (as with RV level sensing for midloop operations at many PWRs). For most plants, technical specification limiting conditions of operation (LCOs) associated with the availability of equipment do not exist during outages. In addition, operators and other (sometimes transient) plant personnel make many more manual interventions with the plant, so there are more opportunities for EOCs that create unusual plant failure modes. The unusual failure modes, in turn, create new opportunities for error.

Beyond these very general aspects of plant conditions are the more direct task-relevant conditions. For example, the failures or deficiencies of temporary level instrumentation played a significant role in events, as discussed in several evaluations of LP&S events, including NRC's NUREG-1449. This particular plant condition is considered different from the PSF of human-system interface because it is the condition of the plant that renders the instruments deficient. System failures of instrumentation have the potential to cause multiple unsafe actions because they create a false perception in the minds of the operators about plant conditions. This can cause operators to take inappropriate actions, from which it can be difficult to recover.

5.5 Analysis of Dependencies in Event Data

Appendix C gives a detailed analysis of the incidence of dependence mechanisms identified in reports of events. The following is a summary of this analysis.

Both LER and the NRC's more detailed AEOD and AIT event reports were reviewed to identify dependence mechanisms associated with multiple unsafe actions. Because of the limited descriptions in the LERs, no dependence mechanisms were identified in the relatively few events involving multiple unsafe actions.

Seven LP&S events were described in either AIT or AEOD human performance studies. In five of them, multiple unsafe actions were identified. With one exception, dependence mechanisms were identified in these events (Appendix C). Table 5.2 summarizes these events, and the findings on dependence mechanisms.

Table 5.2 Review of AIT and AEOD Human Performance Study Reports

Plant/Event Data	Number of Unsafe Actions	Dependence Mechanisms Identified
Braidwood Unit 1 (12/1/89)	2	common process: procedures
Diablo Canyon Unit 1 (3/7/91)	2	common PSFs: communications, organizational factors
Oconee Unit 3 (3/8/91)	3	common PSFs: procedures, organizational factors
Crystal River Unit 3 (12/8/91)	2	common PSFs: procedures, stress
Catawba Unit 1 (3/20/90)	2	none identified
Braidwood Unit 1 (10/4/90)	1	none - one unsafe act
Prairie Island Unit 2 (2/20/92)	1	none - one unsafe act

5.6 Dependency Conclusions

The evaluation of operational event data in the AIT and AEOD reports indicated that the majority involve multiple unsafe actions for which there are dependence mechanisms. In the event descriptions in LERs, there was insufficient information to identify separate unsafe actions, or the existence of dependence mechanisms. The limitations in LER reports as a basis for HRA modeling were discussed in NUREG/CR-6093 (Barriere et al., 1994b).

Based on the research efforts, a useable and useful taxonomy of dependence mechanisms, associated with specific causes, was demonstrated to aid in the analysis of operating events and the structuring of data relevant to human reliability. This taxonomy will allow dependence mechanisms to be explicitly considered in PRA modeling, and quantification stages to be developed in the next phase of this project. In the interim, we suggest some simple rules for modeling human failure events in PRAs.

These simple rules provide an initial basis for assessing the dependence between multiple human failure events in PRA models; they will be re-assessed when we extend the database and develop the quantification methods during the next phase of the project. These rules are "crude" in the sense that they are basic and, at this stage, do no more than bound the potential for dependencies on the basis of the observed events.

(1) Dependence between unsafe actions should always be assumed initially. Independence requires that even if the actions are well separated in time, there are:

- no common procedures,
- no common PSFs,
- no common hardware, and
- no common personnel.

The sparse reporting of dependencies in the LERs is seen more as an omission in the reports, than as an absence of dependencies in the events. Of the five AIT or AEOD reports identifying more than one unsafe act, only one did not identify dependencies.

(2) Any initiating event that is instrument-driven will have adverse effects in the recovery phase. There are numerous examples where a flawed instrumentation system induced operators to initiate an accident, and subsequently limited their ability to diagnose the accident.

(3) Operations that are not conducted in accordance with the intentions of planners or supervisors reduce the ability of operators to terminate problems. Such operations were reported during LP&S operations, as in the case of the loss of RHR at Catawba Unit 1 (3/20/90).

6. INDEPENDENT PEER REVIEW

6.1 Peer Review Process

After the technical completion of the project's Analysis and Characterization Phase (mid-January 1994), an independent review of the project's progress was held at NRC offices on February 8-9, 1994. The review included a one and a half-day presentation of the research and results by the BNL project team, followed by a half-day session of reviewers' questions, clarifications and comments. The participants included the NRC/RES/Division of Safety Issue Resolution management associated with the project and other NRC representatives from RES/Human Factors Branch, NRR/Human Factors Assessment Branch, AEOD/Trends and Patterns Analysis Branch, and NMSS/Industrial and Medical Nuclear Safety Branch. In addition to NRC management and staff, six non-NRC reviewers participated in the review. They were invited because of their involvement in related work, and included representatives from universities, national laboratories, and independent consultants.

Before the meeting, each reviewer received a package containing updated versions of the reports developed during the Analysis and Characterization Phase. The actual documentation is included as Appendices A, B, and C of this document, respectively entitled "HRA Framework Refinement," "Identify and Represent Errors of Commission," and "Develop Approach to Deal with Human Dependencies." As part of the review, each participant was asked to respond to four questions posed by the NRC project management:

(1) Is this HRA approach technically valid?

(2) What is the regulatory utility of this work?

(3) Is the new approach to HRA useful to PRA?

(4) What modifications and recommendations should be considered in moving forward with the HRA Development Process Phase?

At the close of the meeting, each reviewer gave initial verbal feedback. This was followed soon after by written comments and recommendations from each reviewer to the NRC Project Manager. Following a review by the NRC project management, the written comments were sent to the BNL project team who then made a detailed evaluation and categorization of them. The comments and recommendations are summarized below.

6.2 Summary of Reviewer Comments and Recommendations

In general, the reviewers expressed positive confirmation of the Analysis and Characterization Phase and its potential applications. In response to the above questions, they reported that the approach was valid, of extensive utility to NRC, and useful to enhancing the PRA process. Worthwhile guidance also was given to the project team in the form of recommended modifications and additions for future efforts. The reviewers' comments and recommendations were categorized into five potential areas of expansion. The following discussion summarizes the reviewers' recommendations for each potential area of expansion (i.e., in response to question 4 above): (1) developing a database protocol, (2) expanding the HSECS database, (3) expanding the framework, (4) developing user guidance for the framework, and (5) address-

ing validity and benchmarking issues. The reviewers' recommendations on the applicability of the project's accomplishments to other NRC activities are summarized in Section 6.3.

6.2.1 Database Protocol Development - Reviewers' Comments

Most reviewers said that it would be useful for the project team to develop a protocol to guide the use of the proposed HSECS database. Recognizing its potential utility, several reviewers indicated that a protocol would help, for example, incident investigators determine the root cause(s) of human error and assist the NRC (e.g., AEOD) in analyzing human-performance data and creating an agency-wide human-performance database. Many reviewers further commented that a protocol for analyzing event data in the context of the framework would significantly enhance the value of the database by making analyses more objective, and therefore, more repeatable and consistent.

One reviewer reported that "...a major challenge (to HRA quantification) is to be able to identify a few dynamic "story-boards" that describe the essentials of a relatively large number of events. Fortunately, both the event data and the framework indicate that this distinct possibility can be realized by further data analyses, guided by a developed protocol and expanded framework." Another reviewer indicated that "...to establish (HRA) rules you need theoretical underpinnings which could be realized by a protocol to provide guidance for detailed event analyses."

6.2.2 Expand HSECS Database - Reviewers' Comments

The reviewers expressed a strong consensus on the need to base HRA/PRA improvements on operational data; for example, the need for the project team to expand the current database (i.e., increase sample size) by applying the framework to analyze additional human performance operational data. As one reviewer pointed out, "...the review of a relatively few critical events does not constitute a valid or reliable empirical base for predicting relationships among framework components..."

Many reviewers indicated that the data review should be carried further to look at more LP&S events, events that have occurred during full power operation, and successful performance in events, to better glean information about important PSFs. It was recommended that a closer look be taken at which factors were really important influences on human performance, i.e., what factors actually led to human failure. One reviewer pointed out that "...the ability to explain what is required in terms of the type of PSFs and how many must be deficient in order to lead to different types of error mechanisms has not yet been performed. The sample size is too small and it is important that more events and data sources be analyzed." Another reviewer also stated that "...there is a need to clarify a better class of PSFs because current PSF schemes are vague (e.g., training - that is, "less than adequate"). More objective PSFs, whose strength can be determined or inferred from an event report, need to be determined from more detailed and/or additional event analyses."

In addition to clarifying the influence of PSFs on human performance, several reviewers reported that the framework and additional data analyses need to address other "major non-trivial" issues including the dynamic nature of human-system interactions, the presence of teams of operators, and knowledge-based performance; to address these issues, many reviewers identified potentially useful sources of information (i.e., beyond NPP event data). As one reviewer pointed out, "...the main purpose in expanding the database is to provide more data to help understand the factors that govern human behavior; i.e., PSFs, plant conditions, organizational factors, etc. Consequently, there is no reason to restrict the data to the

nuclear industry, in fact, much can be gained from reviewing other industry data including chemical processing, military and transportation."

Additional recommended sources of data included: French LP&S and/or simulator experiments; FAA, DOD, and NASA human reliability data; and railroad industry incident investigation data. One reviewer indicated that the project team "...may want to consider the empirical data offered by the behavioral sciences field (e.g., cognitive psychology - Christopher Wickens, Mica Endsley). Integrating the data from cognitive and aviation psychologists may prove useful in determining, for example, why problem solving and decision making failures (mistakes) occur in complex environments."

6.2.3 Expand HRA Framework - Reviewers' Comments

Most reviewers indicated that the next phase of the project should continue developing the framework and applying it to describe and analyze additional human performance data. These comments can be best represented by a distinction between (1) expanding the framework to clarify relationships and linkages between framework elements, and (2) developing the framework into a tool to explicitly support the improved HRA quantification process. Recommendations for these two aspects of framework expansion are discussed below, respectively.

Expanding Framework Elements

Several reviewers commented that the framework elements should be expanded to accommodate, for example, the three identified characteristics of major accidents, the dynamic nature of human-system interactions, and the presence of teams of operators. Another reviewer pointed out that "...the present framework should better represent how people process information, knowledge-based performance, the influence of situation awareness, the importance of workload or the acknowledgement of workload transaction as a factor leading to errors for human performance in complex situations."

As one reviewer stated "...there is a considerable gap between current HRA practice and contemporary views about the psychological, situational, and organizational influences upon human unsafe acts. The framework has the potential of providing, for the first time, a theoretical underpinning that is rich enough and yet modelable to bridge this gap. While the current framework does address key driving forces in both the personnel and the plant and reflects the right theoretical elements, it still needs to be expanded in order to clarify their interrelationships (e.g., between elements). More has been provided than could ever be accommodated in HRA. But this is necessary at this stage. In addition, the project team needs to clarify the fuzzy edges between organizational factors, PSFs, and plant conditions. For example, what are the causal relationships between organizational factors on the one side and the moderating influences of plant conditions and PSFs on the other?"

Another reviewer indicated that "...the framework is good for characterizing error mechanisms, unsafe acts, and human failure event (HFE) processes, maybe the most cogent around, but there are no established rules regarding human performance; e.g., why some crews overcome procedural inaccuracies and why others fail hopelessly. In addition, we do see from the events, that crews during LP&S and in significant other events 'work outside the rules [design intention], don't understand the regime that they are in, and ignore or dismiss evidence being presented to them.' While this is a very worthwhile set of clues regarding human performance, future efforts should focus on what conditions induce crews to perform in any or all of these three failing manners."

Develop Framework to Support HRA Quantification Process

Several reviewers reported that while the framework currently can provide a common working language, it may not have a home in conventional methods of quantification, and has not yet established several rules necessary before quantification can proceed. It was further suggested that by improving the validity and usefulness of the data and by identifying appropriate causal mechanism linkages as identified by the framework, "the potential exists for providing an integrated transition model to quantification, i.e., the rule set of which PSFs lead to error mechanisms and in what contexts produce unsafe actions leading to human failure events."

One specific recommendation was for the project team to "...think about the quantification model (even a crude one) as soon as possible, so that the framework will not get out of hand. For example a great deal of detail that the framework has now may not be utilized. Furthermore, before proceeding with the quantification development process, 'statements' should be made regarding which aspects of the framework are explicitly tied to the quantification methodology, and any presumed relationships should be demonstrated [i.e., supported by the data]."

Another specific recommendation was that "...the framework should be more like a process diagram that illustrates how the probabilities of human failure events found in a PRA might be calculated." One reviewer suggested that consideration be given to "a framework origin that stems from the plant state (i.e., as described by the PRA) to define the context for the HFEs, then branch out to consider the relevance and importance of the various framework elements. Ultimately, it is the status of the plant that needs to be considered; i.e., what went wrong, under what conditions, and what was the HFE or events that contributed to the undesirable plant conditions. Consequently, what was it about the plant state that contributed to creating the context for the human failure?"

6.2.4 Develop Framework User Implementation Guidelines - Reviewers' Comments

Many reviewers reported that the NRC could benefit from a qualitative technique, with associated guidance, that could easily, thoroughly and reliably enable an analyst to identify and describe human performance and error, as well as their causes and potential solutions to prevent or mitigate the error. Focusing on developing the framework as an "evaluation and analysis tool," was considered an important endeavor in addition to using it in the new HRA quantification methodology.

It was pointed out that additional guidance is needed as to how an analyst should use the framework. As one reviewer stated, "framework implementation guidelines will enable "experts" to gain an understanding of the important framework elements (i.e., subcomponents like particular PSFs or plant conditions) and their inter-relationships, and thereby provide guidance on what to consider in an expert elicitation process. It would also enable specific examples of component relationships (i.e., supported by the data and consistent with theoretical underpinnings) to be provided."

Another reviewer pointed out that, "while the framework identifies recurrent patterns of cause and effect over several events, this can only be done effectively if the analysts are committed to a common theoretical framework. The project offers such a framework: user guidelines would facilitate its proper use."

Finally, it was recommended that framework guidance should include a set of questions "to guide the review and implementation of the framework. Questions must be along the lines of what type of errors

have occurred and where must the crews be in their thinking, in order for proposed clusters of PSFs or single PSFs to induce, for example, EOCs (that is, what makes them or other error types more susceptible?)."

6.2.5 Address Validity and Benchmarking Issues - Reviewers' Comments

Several reviewers requested that the project team take validity, and a review of the state-of-the-art in HRA much more seriously, to facilitate its acceptance amongst analysts and practitioners as much as possible. One reviewer reported that, "an invalid quantification methodology that purports to be better than existing methods because of all the behavioral factors it considers, could do more harm than good. Furthermore, since relevant data will be scarce, the validity of any methodology will be difficult to demonstrate. However, given the existing "state-of-the-art," any straight forward, systematic approach that at least has some degree of demonstrated validity, would be very useful."

It was suggested that to provide a sounder basis for validity (i.e., in addition to an expanded database) good literature to consider included: the ISPRA research group under Carlo Cacciabue - "COSIMO: A Cognitive Simulation Model of Human Decision Making and Behavior in Accident Management of Complex Plants" (Cacciabue et al., 1992); research conducted at INEL - "INTENT: A Method for Estimating HEPs for Decision Based Errors" (Gertman et al., 1992); and the ISPRA Benchmark Exercise (Pouchet., 1988). It was further suggested that it would be useful to address the reasons for a wide scatter of results in implementing HRA methodologies, e.g., as identified by the ISPRA Benchmark Exercise.

It also was suggested that the literature in the behavioral science area should be reviewed (in addition to an HRA methods and expert elicitation literature review) and that the empirical data offered by that field (e.g., information processing and other similar psychological perspectives) should be considered.

6.3 Regulatory Applications Identified by Project Reviewers

The following discussion summarizes independent reviewers' comments, from both NRC and non-NRC participants, about the regulatory usefulness and potential application of this work. These are additional comments and recommendations to those discussed above, which were primarily related to expanding/modifying future project technical development. These suggestions do not impact specific Development and Implementation Phase efforts; however, they are excellent recommendations that may be further considered in supporting other NRC activities.

The following are the recommendations adopted from the independent reviewers written responses made to the NRC project management.

- The HSECS database should assist NRC in their on-going efforts to gather and analyze data on human performance, and aid in the development of an agency-wide human-performance database. The most immediate application is providing NRC analysts with tools for understanding event reports from the perspective of human performance.

- An expanded representation of events in the HSECS database can potentially facilitate future NRC queries regarding, for example, whether automation of selected portions of LP&S operations could help avoid the kinds of events that have occurred.

- The approach to diagnose the causes of significant events involving human performance deficiencies should be particularly useful in improving guidance on future requirements for Licensing Event Reports (LERs).

- The proposed integrated HRA/PRA framework could be useful to NRC in analyzing operating experience and could support Diagnostic Evaluation Teams in assessing plant management and operations by helping incident investigators determine the underlying causes of human error.

- The framework could be a useful interface with the NRC/RES organizational factors research program, particularly in identifying significant organizational factors which potentially impact plant conditions and PSFs, and thereby, influence human performance (e.g., unsafe actions).

- The framework may reveal potential risk-significant situations, and may assist analysts in deciding how to respond to problems by enabling them to think about human reliability in a more systematic, integrated fashion.

- The framework provides a consistent way of structuring investigations so as to elicit key human-factors issues. Consequently, the NRC should consider extending the insights offered by this program into the field of event investigation and analysis, and using the framework and database to identify recurrent patterns of cause-and-effect over several events.

7. RESEARCH IMPLICATIONS

The basic concepts of the improved process for HRA are in place, having completed the Analysis and Characterization Phase. These concepts have served as the basis for retrospective analysis of real operating-event histories, which has identified the context in which severe events can occur; specifically, the plant conditions, significant PSFs, and dependencies that "set up" operators for failure. However, using the framework for prospective analysis, i.e., defining the context so that important EOCs and dependencies can be identified and predicted, remains to be specified. As Hollnagel (1993) points out, this process must constrain the vast space of possible unsafe acts and permit practical analysis.

To accomplish this objective and provide an improved approach for HRA, the implications of the research efforts discussed in the previous sections need to be identified, integrated, and discussed. The subsections below describe these research implications with respect to the following:

1. further use of the framework for integrating research and development efforts;

2. specific details and insights on EOCs and dependencies;

3. the need for improving the database, particularly in capturing an extended representation of unsafe actions, their associated contexts (e.g., plant conditions, PSFs, dependencies), and event timelines;

4. the specific limitations of HRA that become apparent from our current understanding of human performance; and

5. development requirements that must be resolved in the project's remaining Development and Implementation Phases to accomplish an integrated HRA/PRA methodology.

7.1 Framework Implications

As discussed, the Analysis and Characterization Phase included: (1) the development of a multidisciplinary framework for better integrating HRA with PRA; and (2) the characterization of EOCs and human dependencies, including general guidance for their identification and representation in PRAs. The following discusses further implications on the framework's role in supporting the modeling of EOCs and dependence mechanisms, as well as its potential utility in further integrating the continued development of the project.

The framework represents an important accomplishment of the Analysis and Characterization Phase in that it provided an orderly rational structure for considering human-systems interactions in NPP safety. Concerns that HRA techniques do not represent realistically the roles that humans play, both in creating and preventing accident conditions, had been identified in several evaluations of PRA technology, including the NRC's PRA Reference Document (NUREG-1050, 1984). The development of an explicit framework of how the disciplines of human factors, behavioral science, plant engineering, HRA, and PRA are related, was needed to be able to identify the necessary document requirements for HRA.

The framework was developed from our the review of significant operational events. Therefore, new developments in HRA now will be better able to represent real-world human performance. Further refinements will be necessary as additional operational events are reviewed, new knowledge is developed

in the fields of human factors and psychology, and new needs are identified in PRA. This requirement is to be welcomed, not feared, because a framework that can grow with needs and knowledge will be a great advantage in the future. The framework provides the basis for discussing many different factors that impinge on human-system performance, not just those employed in a single technical discipline, such as human factors or plant engineering.

To better address current HRA concerns, the framework had to describe the relationships between PSFs, human error mechanisms, unsafe actions, and plant conditions. In addition, for integration into the PRA, the framework needed to identify the relationship between human failure events, associated PRA models, and plant states (i.e., as defined by the PRA). By identifying such linkages, the human contribution to risk and the salient characteristics of severe accidents can be described more explicitly.

Retrospective analyses of operational events showed that the framework can identify factors that influence humans to perform unsafe actions, and provides a systematic basis for evaluating the significance and characteristics of EOCs and dependence mechanisms. Thus, the framework enables important aspects of EOCs and dependence mechanisms to be considered in developing an improved HRA methodology, and clarifies the requirements for their more realistic inclusion in PRA models. The framework's provision of a common language and structure, for relating the different dimensions of human-system interactions, permits evaluations of EOCs and dependencies that are both tractable and tenable. Considering the importance of these issues in NPP safety, this change is an important advance. These EOC and dependency capabilities are expected to be refined and expanded subsequently in the project.

Once the structure and terminology were defined, use of the framework encouraged organization of the facts in a way that clarified important insights from the analysis of significant operational events at plants; i.e., a reframing took place, that permitted analysts to see important structure that previously was hidden. One example is the identification of the three characteristics of severe accidents (in Section 2). Event analyses also played a dominant role in understanding the factors surrounding the occurrence of EOCs and multiple dependent errors. Indeed, identifying the factors surrounding these errors would be extremely difficult without the ability to analyze the events systematically using the framework. After such analyses, it became apparent that improvements in the database were needed to better characterize human actions and their associated performance context (e.g., in terms of significant plant conditions, PSFs, and dependencies), and to better describe the timeline of an event. These database needs are further discussed in Section 7.3. The Stockholm Workshop (1994) also identified the consideration of context, and its associated database implications, as one of, if not the most important improvements needed in next generation HRA methods.

We anticipate that the continued use and expansion of the framework and its applications in considering EOCs and dependencies will provide a rational basis for estimating error probabilities, and incorporating human failure events into the PRA process. While the details of these activities are still under development, the systematic structuring of the different dimensions influencing human-system interactions, brings a degree of clarity and completeness to the modeling of human errors. The lack of this systematic approach has limited the ability to incorporate human errors in PRAs in a way that could satisfy both the engineering and the behavioral sciences. Consequently, the results of PRAs have lacked credibility in terms of their representation of the contribution of human errors to power plant safety, particularly when compared with the experience of major NPP accidents and incidents where human error has proved to be the dominant factor. Without the explicit, realistic representation of human-performance characteristics identified in real events, PRA can only partially reflect the causes of risk.

7.2 Errors of Commission and Dependence Mechanisms Implications

A major goal of this project was to appropriately model and quantify EOCs and dependence mechanisms, which are of concern because they were found to be involved in significant operational events. The following discussion describes the implications of these EOCs and dependencies and how to bound a search for them.

In the context of PRA, identifying the potential opportunities for EOCs required first identifying those of concern. The simple definition of an EOC is clear - *an overt, unsafe act that, when taken, leads to a change in plant configuration with the consequence of a degraded plant state*. However, to support PRA, a structure for classifying EOCs is needed to limit the search to important events, not previously modeled.

Section 4 identified the concept of an "EOC" as a characteristic of PRA and plant-operations thinking, not a characteristic of human behavior. In the PRA sense, EOCs are any inappropriate human action(s) (i.e., slip, lapse, mistake, or circumvention) performed that does not follow the most direct route to system success mapped in the procedures, under an assumed accident progression. There are a potentially unlimited number of such EOCs. To organize our thinking toward setting boundaries for this unlimited potential, Figure 7.1 groups EOC human failure events into categories relevant to the PRA model; that is, EOCs that produce isolated (i.e., independent) effects versus dependent effects. An isolated effect has no coupling with later hardware demands or human actions. The figure also gives suggestions for modeling EOCs and the use of data. Based on the following discussion of Figure 7.1, it will be shown that contrary to current perception, many EOCs (i.e., those with isolated effects) are already considered in PRAs.

As illustrated by Figure 7.1, EOCs with isolated effects include both initiating events, and events that impact equipment unavailability. The EOC initiating events are modeled in existing PRAs. Typically, lists of initiating events are developed on a functional basis, independent of cause (human or hardware). The fact that they may be caused by EOCs generally, is irrelevant for events with no dependent effects. However, analysis of the data may still be worthwhile if the EOCs are identifiable in the initiating event data, e.g., to understand and quantify EOCs for other settings.

For initiating events, which occur so frequently that their occurrence appears in PRA initiating event databases, these data could be examined to see if it is possible to determine which specific ones were caused by human EOCs. If identifiable, and if the context of each event can be established, such information could be helpful in quantifying the frequency of other modeled EOCs (e.g., for setting boundaries on the frequency of challenging conditions). If there are no such identifiable instances of EOCs causing particular initiating events in the PRA initiating event databases, the initiating event lists can be considered independent and complete; i.e., there are no required searches or conceptual problems. For rare initiating events, with frequencies based on modeling, not data, it would be advisable to review the possible contribution from EOCs not yet modeled.

EOCs with isolated effects on equipment unavailability (such as stopping an individual pump or closing a normally open valve) are generally included in the data on equipment failure rates. As for initiating events, the failure data could be examined to see if it is possible to determine which specific events were due to human EOCs. If identifiable, and if the context of each event can be established, such information

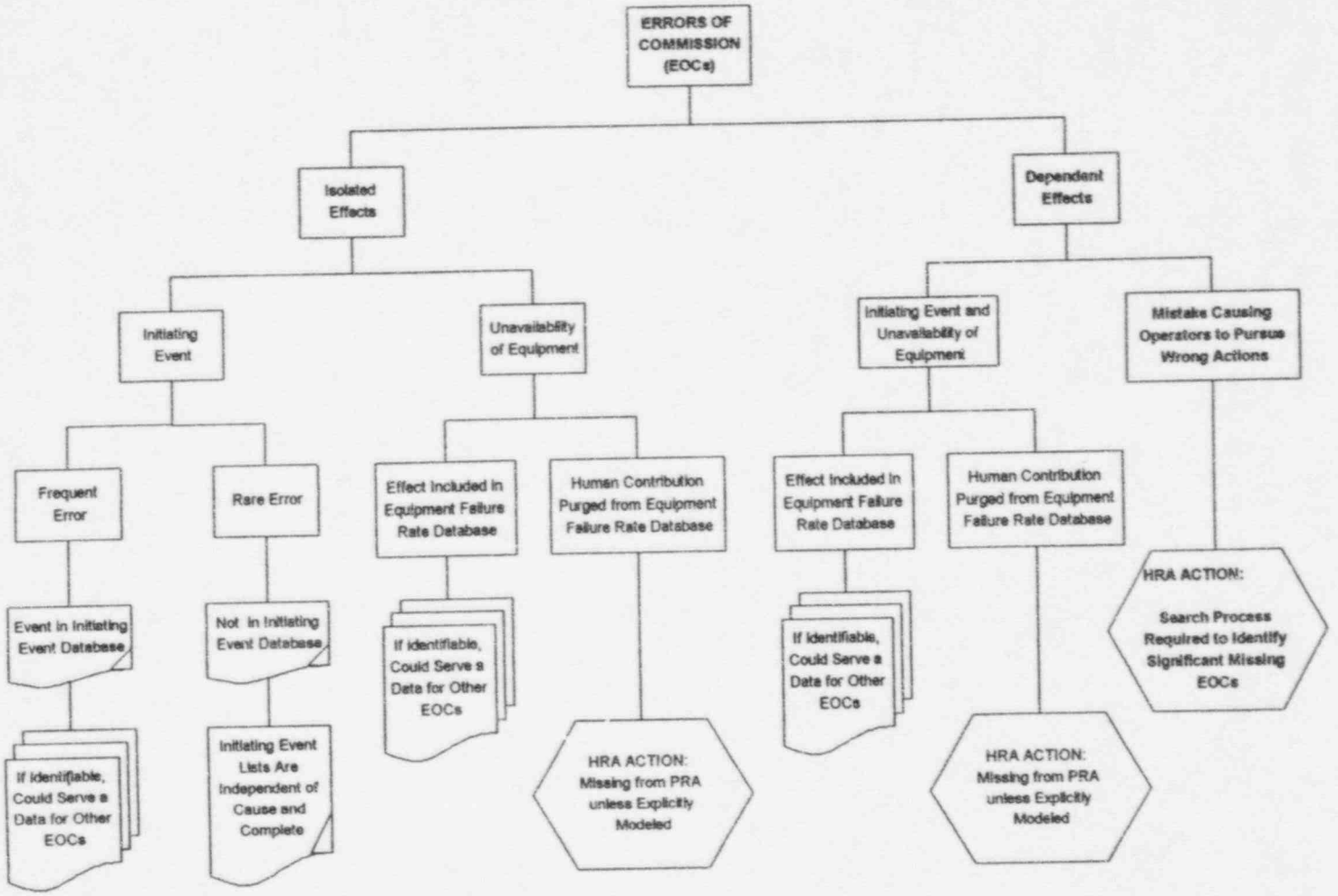


Figure 7.1 Categories of errors of commission

could again be helpful in quantifying the frequency of other modeled EOCs. If such events have been purged from the data, explicit modeling in the systems analysis will be required to restore completeness. In summary, EOCs with only isolated effects generally are modeled in existing PRAs, and with few exceptions, only limited application of existing techniques should be required to ensure proper treatment.

The dependent effects illustrated in Figure 7.1 are more problematic because initiating events involving dependencies can affect the PRA in two ways. On the left leg under dependent effects, the initiating event also affects systems required to mitigate the accident, but does not impact subsequent human actions. This should (in most cases) already be included in the PRA modeling process for common-cause initiating events (as in the case of external events). The fact that the event was caused by an EOC is not important. A more serious case, and a principal development focus from this point onwards, involves an EOC that is coupled to subsequent human actions, as shown on the right leg under dependent effects. An example of an EOC with dependent effects is a mistake that sends operators pursuing an incorrect response during an accident. Another, may be a circumvention that produces unexpected misunderstood plant conditions. The immediate EOC may be a slip, but if so, it is followed by the mistake of believing that no slip occurred. That is, the operator "knows" that the action was carried out correctly (in his mind, at least)!

Based on the above discussion, out of the range of all possible EOCs, modeling improvements that focus on those leading to dependent effects of other human errors are vital to the completeness and accuracy of PRAs. Consequently, these EOCs require new analysis through improvements in HRA, as described in this report. The others, the isolated events, fit within the framework of those scenarios already modeled in current PRAs. Those that occur frequently should already be represented in the failure data used in PRAs; rare events represent negligible additions to the frequencies used for other events that have a similar effect on the plant.

That the examination has narrowed to EOCs with dependent effects does not mean that the problem is a simple one. Although a large fraction of events in the EOC class have been removed, representing EOCs with dependent effects could still be unmanageable. Thus, the set of EOC events to be evaluated by the PRA must be limited further. Two screening criteria are immediately apparent; consequence and frequency. Any event can be eliminated from further consideration if the dependent subsequent actions have no impact, i.e., consequence, on the likelihood of core damage or on the characterization of the radiological releases (this was previously discussed in Section 4). Any event, whose scenarios are appropriately modeled and cannot contribute substantially to the frequency of core damage or release category, also can be eliminated. These two screening criteria will be incorporated into the EOC search techniques, i.e., procedure and mechanism searches identified in Section 4, in the ensuing development phase of the project.

Improved understanding of the factors that influence the coupling between the EOC and subsequent actions requires a further analysis of the operational event data. Thus, the approach for identifying potential EOC opportunities was developed as an extension of the insights derived from reviewing operating events, and from an understanding of the class of EOCs of significance to PRA. However, the fields in the LACS database, developed as part of the initial LP&S phase of the project, must be expanded to document dependent effects. Events analyzed earlier are currently being revisited to recover this information. The expansion of the database is discussed next.

7.3 Database Improvement Needs

Data analysis has played a large role in our research. The data analyzed influenced the development of the multidisciplinary HRA framework, the modeling guidance for EOCs, and the approach for treating dependencies. As the project evolved, different kinds of data and different perspectives of the analyzed data led to significant insights. The database is expected to provide critical support to future tasks, including the use of descriptive information from the database in the quantification process.

Several necessary improvements to the HACS database (Barriere et al., 1994b), have been identified, related principally to the evolution of the project, our current understanding of human performance, and the associated unanticipated needs of research and development (e.g., framework, EOCs, and dependencies). Consequently, it is important to update and improve the structure of the database scheme and user-interface to support current and future work.

The most notable improvements to the HACS database scheme and structure are needed to address:

- difficulties in accommodating the more useful, detailed information contained in event-based reports, such as USNRC AEOD Human Performance Studies and Regional Augmented Inspection Team (AIT) Reports;
- incomplete descriptions of essential features of events, requiring analysts to continually return to original documentation to recall important details of events;
- incomplete descriptions of physical conditions of the plant (e.g., system status or configuration);
- inadequate information on diagnosis, diagnostic cues, and associated information required to investigate EOC mistakes;
- insufficient information on common dependence mechanisms (e.g., common PSFs) required to investigate human dependencies; and
- inadequate information on the timing of human actions and hardware failures and actuation.

To address these issues, a new database scheme structure and user-interface will be developed in the next phase of the project. It will support future analyses of operational events and will be designated the Human-System Event Classification Scheme (HSECS), to emphasize the significance of real human-system interactions in operational events. A continuing theme from this work is that very detailed reports, from multi-disciplinary reviews performed immediately after serious events, provide the richest source of information for improving next-generation HRA methods. The Working Group on Data at the International Workshop on Advanced Topics in Reliability and Risk Analysis: *Theoretical and Practical Challenges*, in Stockholm, Sweden, August 1994, came to the same conclusion. After discussing the types of data available, the group reached consensus that only the detailed multidisciplinary reports, such as USNRC Regional AIT and Incident Investigation Team (IIT) Reports, and AEOD Human Performance Studies can support the needs of developing HRA methods, that will attempt to accommodate models from cognitive psychology and other behavioral sciences.

A preliminary example of the anticipated future HSECS database structure is given in Attachment 1 for the 1991 Oconee Unit 3 event (as reported in USNRC AEOD and AIT reports). The structure used in

the example, which addresses the above issues, illustrates several intended modifications to the HACS database structure.

1. The capability to store additional information on plant conditions to aid database users in discerning, for example, salient plant conditions before and after the event.

2. A new naming scheme to differentiate between unsafe acts (U), non-error human actions (H), equipment failures (E), and recovery actions, and the capability to collect performance-shaping factor (PSF) information for each.

3. PSF information is expanded to include: (a) both positive and negative influences, and (b), important event-specific illustrations.

4. Addition of fields related to diagnosis (and associated instrumentation) and to dependencies between unsafe acts.

5. Graphics included to better illustrate key features of the event. In particular, an event timeline showing the sequence of human and equipment events and illustrating dependencies between unsafe actions. Also, a simplified system drawing to aid in understanding the progression of the event.

6. Revisions to the format of database displays to make information more readable.

Some sources of event data may have insufficient information to use several of these new features. For example, many LERs do not contain adequate information to identify dependencies, develop a diagnosis log, or draw a simplified piping and instrumentation diagram (P&ID). However, the new database structure will be flexible enough to accommodate a variety of data sources, and make better use of the information available from those sources that provide a substantial amount.

7.4 Implications for Addressing Current HRA/PRA Limitations

The broad implication of the work completed to date is that PRAs can more realistically reflect NPP risk by considering multidisciplinary HRA framework elements, especially those related to EOCs and human dependencies. Analyses of operational events, predominantly for LP&S conditions, have shown that: (1) UACs occur frequently and include human-induced initiators, (2) mechanisms for human dependencies based on plant conditions, common PSFs, and common organizational factors can play an important role in the development of an event, and (3) human performance is significantly influenced by the combination of PSFs and plant conditions.

However, the theories of human error underlying the multidisciplinary HRA framework only broadly explain why unsafe acts occur. Similarly, the investigations of EOCs and human dependencies give limited understanding of why specific events have occurred. What remains to be done is to identify, define, and characterize those additional human failure events that should be included in PRA models by re-examining and modifying current HRA/PRA modeling assumptions, conventions, and techniques in light of the insights gained by analyzing event data using the multidisciplinary HRA framework. The following subsections highlight some limitations in current HRA and PRA methodologies that became apparent from the project's research, and discuss some requirements necessary to remove these limitations.

7.4.1 Current HRA Limitations

Current HRA methods recently have been criticized for their inadequate representation of EOCs and human-error dependencies, both for modeling and quantification. The problem for HRA/PRA analysts can be summarized as a lack of guidance in identifying and representing EOCs and dependencies in PRA models, and for explicitly modeling and quantifying the new plant states these errors can create, and the PSFs that influence their occurrence. Fragmented efforts at development have generated separate non-integratable models, which reflect a lack of communication among disciplines relevant to human error in NPP operations, such as human factors, behavioral science, and plant systems engineering.

Another reason for the criticisms is that existing techniques are often inconsistent with "real world" human errors because, for the most part, they comprise "decompositional" models that do not realistically represent realistic human performance, and consequently miss the important synergistic implications of human reliability. In addition, methods typically are not based on actual NPP operating experience and do not explicitly consider the context in which humans are performing.

Previous reports indicate that, for the most part, humans are reliable except when forced into failure by particular plant conditions, inadequate PSFs, or most often, a combination of both. The significant influence of plant conditions combined with unfavorable PSFs, observed in operational experience, demonstrates that human behavior is highly dependent on other people, as well as on prior unsafe actions.

The project accomplishments (as summarized in Sections 3 through 5) have gone a long way to providing a basis for incorporating these operating experience insights into the PRA. However, we recognize that specific developments are necessary so that HRA and PRA analysts can benefit from these accomplishments through a working integrated HRA/PRA methodology.

7.4.2 Development Requirements

To remove HRA limitations and put human performance issues into the risk-management setting, better descriptions are needed of how humans cause problems in safety. These descriptions must be derived using appropriate expertise in systems engineering, human factors and behavioral sciences. After this, significant human-system interactions need to be accommodated into PRA logic models. For example, EOCs, dependencies, and more realistic recovery potentials need to be included in fault trees and event trees.

Once event trees and fault trees are adequately defined, human failure events must be quantified more realistically, not only taking into account the significant PSFs, but also relevant plant conditions and the associated dependencies. Such an objective can best be achieved by integrating the diverse perspectives of plant engineering, human factors, and behavioral sciences.

This approach must also accommodate regulatory concerns. As stated in NUREG-1050 (1984): *"...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."* This accommodation should be realized by being sensitive to another critical insight identified in NUREG-1050 (1984): *"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."*

To meet these objectives and also the recommendations of the independent peer reviewers, several specific requirements have been identified:

1. Relate an expanded description of human-system interactions to the PRA modeling process;

2. Finalize the multidisciplinary framework to more explicitly interpret error mechanisms, plant conditions, and circumventions;

3. Develop an extended database that describes and characterizes "real-world" events involving human-system interactions; and

4. Develop an approach for using expert judgment to support modeling and quantification.

Each of these development requirements are summarized below and further discussed in Section 8, Future Plans.

1. To relate an expanded description of human-system interactions to the PRA modeling process, specific changes for PRA logic models must be developed that accommodate an expanded understanding of human-system interactions; i.e., from detailed analyses of operating experience from a multidisciplinary perspective. This will be especially relevant for including EOCs in event trees, for linking multiple failure dependencies in fault trees, and for handling of recovery modeling in both event trees and fault trees.

2. To improve the usefulness of the project's multidisciplinary framework to the overall methods development phase, several improvements are necessary, including more explicit representation of circumventions and their associated PSFs, the development of a taxonomy for plant conditions, and better integration with cognitive psychology. Specifically, the taxonomies associated with plant conditions are expected to be both engineering-related and behaviorally related, and to clarify potential unique influences associated with LP&S, and at-power operations, as well as RCS parameters. Finally, the current classification of error mechanisms will be refined to integrate better with recent applications in cognitive psychology, particularly with respect to the underlying causes of failures in situational assessment and response planning (Roth et al., 1994).

3. To support any achievements made during this development phase, it is important to base them on actual operating experience. Consequently, developing an extended database that describes "real-world" events involving human-system interactions is considered critical. Expanding the database will provide a basis for improving the quantification process by providing operating experience insights that can be described and presented in relation to the elements of the multidisciplinary framework. Consequently, detailed analyses of events will be conducted and will include assessments of time scales of human-system interactions. While the goal is to appropriately analyze about 30-40 events, we realize that each analysis is very labor-intensive. Consequently, the need for collaboration with other potential U.S. and foreign nuclear and non-nuclear data sources and researchers is recognized.

4. The final need is to develop an approach for incorporating expert elicitation for supporting modeling and quantification. For this elicitation process to be effective, it is paramount that it is based on "real-world" experience, interpreted by a multidisciplinary team of experts (e.g., plant engineering, human factors, and psychology). To present real-world experience for

consideration by the experts, a frame of reference manual will be developed, based on analyzed events and operational experience. The expertise required to be involved in the elicitation process includes plant engineering and operations, human error analysis, and PRA. To improve the acceptability of the expert elicitation process, existing ones must be extended. Of equal, if not greater importance, is the need for the process to address specific PRA requirements, including the capability to provide point estimates, uncertainties, and sensitivities.

Section 8 summarizes how these development requirements have been incorporated into appropriate task-related activities for developing an improved HRA method which also accommodates the recommendations of the February 1994 independent peer reviewers (discussed in Section 6). The International Workshop on Advanced Topics in Reliability and Risk Analysis: *Theoretical and Practical Challenges*, in Stockholm, Sweden, August 1994, also outlined an approach for an evolutionary, second-generation HRA method. The project's accomplishments to date (e.g., the use and analysis of operational data) and the development requirements reported above are consistent with the approach outlined there.

8. FUTURE PLANS

The primary objective of the current (FY94-96) Development Phase is to integrate the accomplishments of the earlier project phases and the recommendations of the independent peer reviewers, and to develop an improved HRA/PRA modeling and quantification process that provides the following guidance:

(1) how to identify and incorporate human failure events (HFEs) in the logic models used in PRAs,

(2) what information is required for human error probabilities (HEPs) to be assigned to these failure events,

(3) how to use this information to estimate the HEPs, and

(4) how to incorporate the HEPs into the PRA quantification process.

After completing this phase, the results of the integrated HRA/PRA modeling and quantification will be incorporated into implementation guidelines as part of the Implementation Phase (FY 96). The guidelines will enable non-project team members (e.g., PRA analysts) to implement the developed methodology. The Implementation Phase will also demonstrate the usefulness and acceptability of the guidelines using a suitable PRA.

To guide our Development Phase efforts, document the intended plans for the Implementation Phase, and to meet the above objectives, a detailed program plan was developed and sent to the NRC Project Manager in August 1994. This plan was based on our prior accomplishments and the independent peer review process. Figure 8.1 is a flow diagram identifying the major technical activities included in the program plan. These activities and their contribution to the overall Development and Implementation Phase are discussed in Sections 8.1 and 8.2.

The activities identified in Figure 8.1 will complete the development of the Improved HRA Method Based on Operating Experience and provide implementation guidelines. These activities specifically address the research implications and development requirements detailed in Section 7, and also accommodate the peer-reviewer recommendations identified in Section 6. Furthermore, these activities are consistent with NRC's directions for current and future uses of PRA, set out in the PRA Implementation Plan proposed by SECY-94-219, the PRA Working Group's NUREG-1489 (1994), and the November 2, 1993, memorandum from the NRC Office Directors to the NRC Executive Director of Operations. These activities support guidance for consistent, appropriate uses of the Multidisciplinary HRA Framework and HSECS database, and will make available relevant human performance and operational data for use in PRAs, operating experience evaluations, and risk management activities. In addition, implementing these tasks will better enable the BNL project team to contribute to the three areas for improvement identified by the PRA Working Group, namely; guidance development, training enhancements, and PRA methods development, and also will explicitly address concerns noted in Appendix C of NUREG-1489 (1994) about the lack of universally accepted, valid assumptions on which models are based.

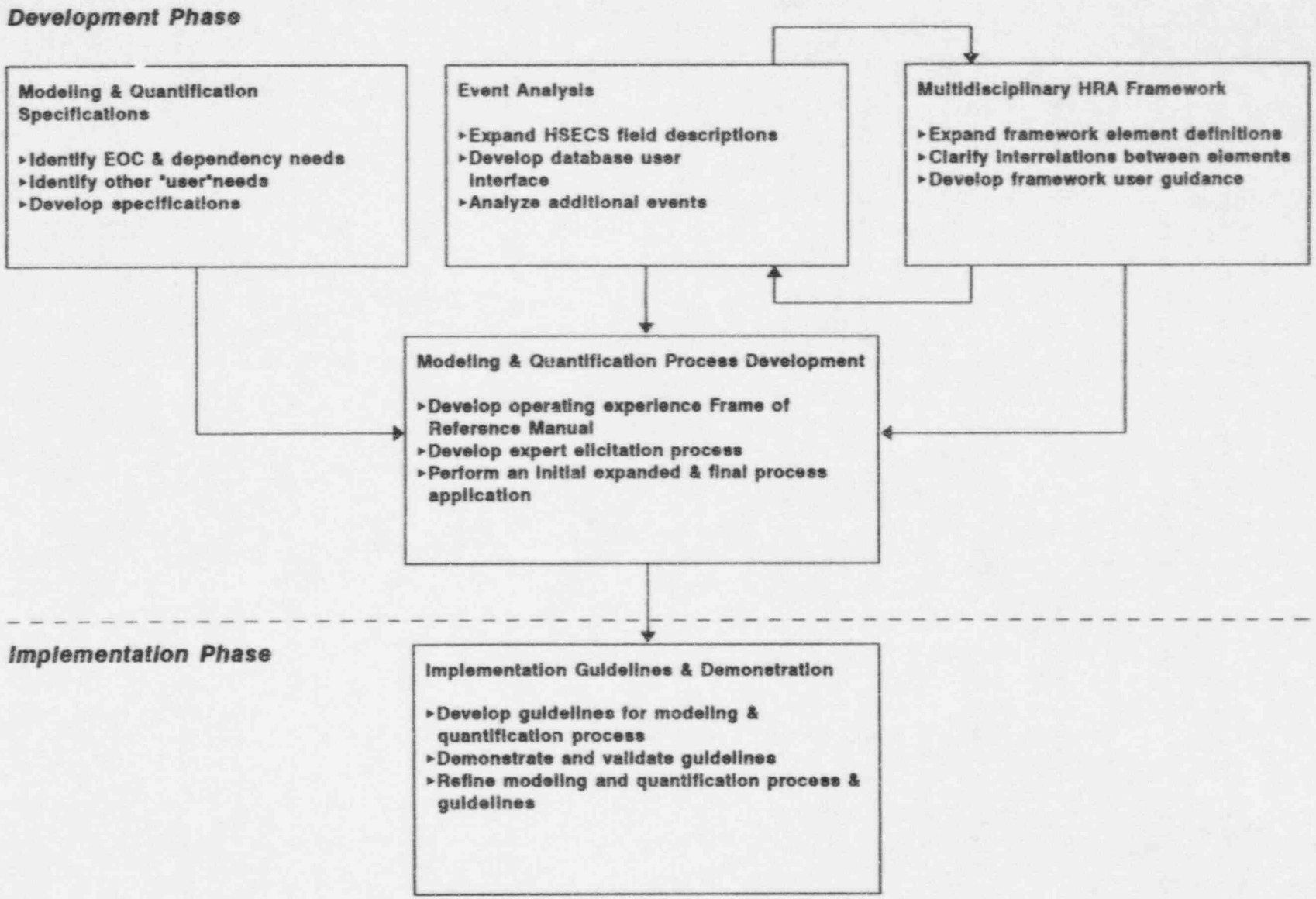


Figure 8.1 Improved HRA development and implementation phase activities

8.1 Development Phase Description

8.1.1 Modeling and Quantification Specifications

To determine EOC and dependency quantification and modeling requirements, their prototypical error mechanisms and associated influences (e.g., PSFs and plant conditions) must be identified, and the final integrated HRA/PRA process must be able to model and estimate their probabilities and frequencies. In addition, issues associated with the quantification of human errors due to constraints and needs imposed by HRA "end-users" need development. As illustrated in Figure 8.1, specifications for meeting these requirements and desired features for HRA improvements will be provided as input to Modeling and Quantification Process Development.

8.1.2 Event Analysis

The database structure of the Human-System Event Classification Scheme (HSECS) will be extended to incorporate new data fields based on insights from event analysis and recent framework developments. An improved user interface and protocol will guide the use of the database through an interactive computer-based format, that will describe and give examples of how HSECS fields are defined and implemented in the context of the multidisciplinary framework. The extended HSECS database and user interface will support additional analyses of events.

The continued analysis of operating events will provide a more empirical foundation to support the proposed framework relationships, as well as a more comprehensive understanding of those factors that significantly influence human reliability. To the extent possible, this expansion will be supported by adding data from detailed, standardized analyses of human performance information from both U.S. and foreign nuclear and non-nuclear sources (including data from simulator experiments). This more comprehensive review and classification of human performance data will provide useful input to the Multidisciplinary HRA Framework expansion and Modeling and Quantification Process Development efforts, which also will help to generate a basis for validation (Figure 8.1).

8.1.3 Multidisciplinary HRA Framework

The expansion of the Multidisciplinary HRA Framework will clarify the definitions of the framework elements, as well as their interrelations and linkages. The specific refinements planned include: (1) a simplified description of human error mechanisms, consistent with recent applications of cognitive psychology (e.g., Woods et al., 1994, and Reason, 1990) that also can be used by the intended community of PRA and plant personnel; and (2) a development of taxonomies for both the operations engineering and psychological aspects of plant conditions, that appear important in creating opportunities for different kinds of error mechanisms. In addition, refinements from event data evaluations incorporating new operating experience findings will be accommodated, as applicable.

As part of this work, two sets of framework guidance will be developed to support the Event Analysis and Modeling and Quantification Process Development (Figure 8.1). The first set will assist analysts in evaluating operational events in a more repeatable, traceable manner, and in applying the elements in the framework to gain a more systematic and complete picture of human performance in events. The second set will support efforts to develop the modeling and quantification process, by guiding the incorporation of human failure events into PRA logic models in a manner consistent with framework concepts, and by clarifying the role of the framework in the expert-elicitation process.

8.1.4 Modeling and Quantification Process Development

An operating experience Frame-of-Reference Manual will summarize the extended database and framework findings, regarding for example, the roles of PSFs and plant conditions in EOCs and the occurrences of multiple dependent errors. The manual will be used in an expert elicitation process to support an improved approach for modeling human failure events, and deriving quantitative estimates of human error probabilities for representative unsafe actions identified from operating experience analyzed in the context of the framework and discussed in the Manual. The elicitation process will build upon proven procedures for systematically eliciting expert opinions, and include a review of such current processes. Consideration will be given to how the Frame-of-Reference Manual should be used to guide expert opinion, and what comprises an adequate spectrum of expertise for effective modeling and quantification.

In support of developing the complete modeling and quantification process, a series of three applications will be conducted and will include modifications to PRA logic models to accommodate new or refined definitions of human failure events (i.e., EOCs). The three stages of development will demonstrate, both within the project and to the NRC, how the expert elicitation process works. This approach will allow refinements at each stage of development, ensuring the viability of the expert elicitation process to incorporate and quantify human failure events in the PRA logic models. The results of this activity will be incorporated into the Implementation Guidelines and Demonstration efforts (Figure 8.1).

8.2 Implementation Phase Description

Implementation Guidelines and Demonstration

The detailed guidelines generated will support the conduct of PRAs which model EOCs and human dependencies and which support the NRC's oversight of the risk associated with human performance in the commercial use of nuclear energy. It is anticipated that the guidelines will enable NRC analysts to carry out a fully integrated HRA/PRA process. These guidelines will provide a hierarchical description of the improved HRA process, as well as the specific methods and criteria necessary to conduct and document each stage in the analyses. Essential requirements for these guidelines are that they: (1) are practical to implement, and (2) produce well-documented, auditable results. Accordingly, the guidelines will be concise and explicit, and contain the tools and data needed for all phases of the analysis.

An evaluation of the implementation guidelines, by a trial application on a selected PRA, will demonstrate the usefulness and understandability of the modeling and quantification process developed, as well as the consistency with expectations and other PRA/HRA results. As part of the demonstration, the developed method will be compared with other accepted HRA methods through a benchmark-type exercise. Any "lessons learned" in benchmarking the guidelines will be incorporated into a revision.

9. REFERENCES

Barriere, M.T., Luckas, W.J., Stock, D.A., and Haber, S.B., *Incorporating Organizational Factors into Human Error Probability Estimation and Probabilistic Risk Assessment*, BNL Technical Report A-3956 3/94, Brookhaven National Laboratory: Upton, NY, 1994a.

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

Bley, D.C. and Stetkar, J.W., *Zion Nuclear Plant Residual Heat Removal PRA*, NSAC-84, Pickard, Lowe, and Garrick, Inc.: Newport Beach, CA, July 1985.

Cacciabue, P.C., Decortis, F., Drozdowicz, B., Masson, M., and Nordvik, J.P., "COSIMO: A Cognitive Simulation Model of Human Decision Making and Behavior in Accident Management of Complex Plants," *IEEE Transactions on Systems, Man and Cybernetics*, No. 22, Vol. 5, pp. 1058-1074, The Institute of Electrical and Electronic Engineers: New York, NY, 1992.

Challenger Accident-Report of the Presidential Commission on the Space Shuttle: Washington, DC, June, 1986.

Chu, T., Musicki, Z., Kohut, P., Bley, D.C., Yang, J., Holmes, B., Bozoki, G., Hsu, C. Diamond, D. Johnson, D., Lin, J., Su, R., Dang, V., Ilberg, D., Wong, S., and Siu, N., *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*, NUREG/CR-6144, Vol. 2, Brookhaven National Laboratory: Upton, NY, June 1994.

Davoudian, K., Wu, J.-S., and Apostolakis, G., "Incorporating Organizational Factors into Risk Assessment Through the Analysis of Work Processes," *Reliability Engineering and System Safety*, Vol. 45, No. 1-2, pp. 85-105, Elsevier Science Publishers Ltd: England, United Kingdom, 1994.

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.

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. 127-137, Elsevier Science Publishers Ltd.: England, United Kingdom, 1992.

Haber, S.B., O'Brien, J.N., Metlay, D.S. and Crouch (Shurberg), D.A., *Influences of Organizational Factors on Performance Reliability - Overview and Detailed Methodology*, NUREG/CR-5538, Vol. 1, Brookhaven National Laboratory: Upton, NY, December 1991.

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

INSAG-1, *Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident*, International Nuclear Safety Advisory Group, Safety Series No. 75-INSAG-1, International Atomic Energy Agency: Vienna, Austria, September 1986.

INSAG-3, *Basic Safety Principle for Nuclear Power Plants*, International Nuclear Safety Advisory Group, Safety Series No. 75-INSAG-3, International Atomic Energy Agency: Vienna, Austria, 1988.

INSAG-7, *The Chernobyl Accident: Updating of INSAG-1*, IAEA Safety Series No. 75-INSAG-7, International Atomic Energy Agency: Vienna, Austria, November, 1992.

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

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

Legasov, V.A., *Memoirs of Academician V.A. Legasov - First Deputy Director of the Kurchatov Institute*, Pravda: Moscow, USSR, 1988.

Medvedev, G., *The Truth about Chernobyl*, Basic Books: USA 1991.

Nader, R., and Smith, W., *Collision Course: The Truth About Airline Safety*, Tab Books: New York 1994.

Nagel, D.C., "Human Error in Aviation Operations," in *Human Factors in Aviation*, (E.L. Weiner and D.C. Nagel, Eds.) Academic Press, Inc.: San Diego, CA, 1988.

NTSB/SS-94/01 (PB94-917001), *A Review of Flight Crew-Involved, Major Accidents of U.S. Air Carriers, 1978 Through 1990 - Safety Study*, National Transportation Safety Board: Washington, DC, January 1994.

NPC(R)-1275, *The Russian Graphite Moderated Channel Tube Reactor*, Nuclear Power Corporation Limited: United Kingdom, 1976.

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

NUREG-1150, Vol. 3, *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, Appendix E.5.1 - "Human Reliability Analysis" (by the H.J.C. Kouts Committee), U.S. Nuclear Regulatory Commission: Washington, DC, December 1990.

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

NUREG-1269, *Loss of Residual Heat Removal System (Diablo Canyon Unit 2, April 10, 1987)*, U.S. Nuclear Regulatory Commission: Washington, DC, June 1987.

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

NUREG-1335, Final Report, *Individual Plant Examination: Submittal Guidance*, U.S. Nuclear Regulatory Commission: Washington, DC, August 1989.

NUREG-1410, *Loss of Vital AC Power and the Residual Heat Removal System During Midloop Operation at Vogtle Unit 1 on March 20, 1990*, U.S. Nuclear Regulatory Commission: Washington, DC, June 1990.

NUREG-1449, *Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States*, U.S. Nuclear Regulatory Commission: Washington, DC, September 1993.

NUREG-1480, *Loss of an Iridium-192 Source and Therapy Misadministration at Indiana Regional Cancer Center, Indiana, Pennsylvania on November 16, 1992*, U.S. Nuclear Regulatory Commission: Washington, DC, 1994.

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

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

Parry, G.W., and Lydell, B.O., "HRA and the Modeling of Human Interactions," in *Probabilistic Safety Assessment and Management*, Elsevier Science Publishers: England, United Kingdom, 1991.

Rasmussen, J., "Models of Mental Strategies in Process Plant Diagnosis," in *Human Detection and Diagnosis of System Failures*, Plenum Press: New York, NY, 1981.

Poucet, A., "Survey of Methods Used to Assess Human Reliability in the Human Factors Reliability Exercise," in *Reliability Engineering and System Safety*, Vol. 22, Nos. 1-4, pp. 257-268, Elsevier Science Publishers Ltd: England, United Kingdom, 1988.

Read, P.P., *Ablaze: The Story of the Heroes and Victims of Chernobyl*, Random House: New York, NY, 1993.

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

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

Rogovin, M., and Frampton, G., *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.

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

U.S. Nuclear Regulatory Commission, Office of Analysis and Evaluation of Operational Data (AEOD), Human Performance Study Report, **Braidwood Unit 1**, October 4, 1990, *On-Site Investigation and Analysis of the Human Factors of an Event (Loss of Coolant During Cold Shutdown)*Washington, DC, October 1990.

..., **Catawba Unit 1, March 20, 1990**, *On-Site Analysis of the Human Factors of an Event (Overpressurization of RHR during RCS Fill)*, U.S. Nuclear Regulatory Commission: Washington, DC, May 1990.

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

U.S. Nuclear Regulatory Commission Generic Letter No. 88-20, *Individual Plant Examination for Severe Accident Vulnerabilities - 10 CFR 50.54 (f)*, Nuclear Regulatory Commission: Washington, DC, 1988.

U.S. Nuclear Regulatory Commission, Regional Augmented Inspection Team (NRC/Regional AIT) Report, **Braidwood Unit 1, December 1, 1989,** *Loss of RCS Inventory via RHR Relief Valve*, Report No. 50-456/89-006, U.S. Nuclear Regulatory Commission: Washington, DC, December 29, 1989.

..., **Diablo Canyon Unit 1, March 7, 1991**, *Loss of Off-Site Power*, Report No. 50-275/91-009, U.S. Nuclear Regulatory Commission: Washington, DC, April 17, 1991.

..., **Oconee Unit 3, March 8, 1991**, *Loss of Residual Heat Removal*, Report No. 50-287/91-008, U.S. Nuclear Regulatory Commission: 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. Nuclear Regulatory Commission: Washington, DC, March 17, 1992.

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.

Whitehead, D.W., Darby, J., Yakle, J., Forster, J., Staple, B., Miller, S., Daniel, S., Brown, T., Walsh, B., Kirk, H., Mitchell, D., Dandini, V., and Benavides, G., *Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1: Analysis of Core Damage Frequency from Internal Events for Plant Operational State 5 During a Refueling Outage*, NUREG/CR-6143, Vol. 2, Sandia National Laboratories: Albuquerque, NM, June 1994.

Williams, J.C., "The MANagement Assessment Guidelines in the Evaluation of Risk (MANAGER) Technique," *Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM)*, Elsevier Science Publishers: New York, NY, 1991.

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

Wreathall, J., *The Development and Evaluation of Programmatic Performance Indicators Associated with Maintenance at Nuclear Power Plants*, NUREG/CR-5436, Science Applications International Corporation: Dublin, OH, May 1990.

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

Wreathall, J., Reason, J.T., and Dougherty, E.M., *Latent Failures and Human Performance in Significant Operating Events*, John Wreathall & Company, Inc.: Dublin, OH, April 1993.

Wright, M., Bellamy, L., and Cox, R.A., "Recent Developments in Chemical Plant QRA," in *Health, Safety & Loss Prevention in the Oil, Chemical & Process Industries*, Butterworth-Heineman Ltd.: Oxford, U.K., 1993.

EVENT NO. INFORMATION

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

Event Date: *3/8/91*
Event Time: *0848*
Plant Type: *PWR/*

Description: *Loss of decay heat removal for ~18 minutes due to loss of RCS inventory via drainpath to emergency sump created by combination of blank flange installed on wrong line & isolation valve stroke testing.*

INITIAL CONDITIONS

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

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

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

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

ACCIDENT CONDITIONS

Other Unit Status:
RCS Conditions:
Power: *Cold S/D*
Temperature(°F): *117*
Pressure: *(head off)*
RV Level: *4' above core*

Other:
* *Loss of 9,700 gal of RCS*

Plant Conditions:
* *14,000 gal. spilled via drainpath to sump (RCS & BWST)*
* *Loss of SDC*
* *Radiation dose rate maximum ~ 8 rem/hr*
* *Local evacuation of areas in RB*

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

Hardware Failures:

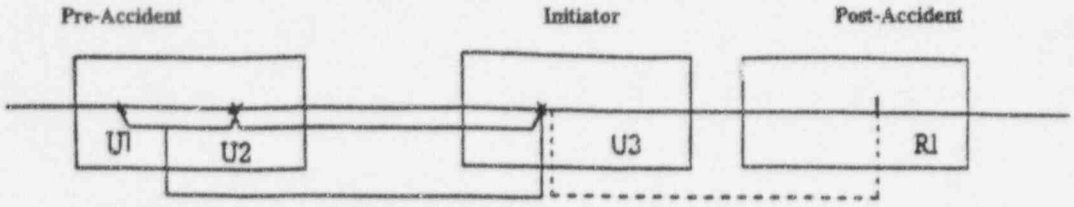
FINAL STATUS SUMMARY

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

Comments: *AEOD report & LER used as sources of information.*

EVENT NO. SUMMARY OF HUMAN ACTIONS

Event Timeline:



Unsafe Actions (U):

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

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

Other Events (Non-Human Error) (E, H, or R):

R1. Operators isolate drainpath, restore RCS level, & restore SDC (including pump venting)

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

EVENT NO. DEPENDENCIES

HARDWARE DEPENDENCIES

System(s) Involved:
Low Pressure Injection (LPI)

Interfacing Systems:
Reactor Coolant system (RCS)

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

Spatial Dependencies:

HUMAN DEPENDENCIES

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

ACCIDENT DIAGNOSIS LOG

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

APPENDIX A

REFINED HUMAN RELIABILITY ANALYSIS (HRA) FRAMEWORK

(FIN L-2415, Task 6)

J. Wreathall, M.T. Barriere, D.C. Bley,
S.E. Cooper, and W.J. Luckas, Jr.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

A.1 INTRODUCTION

A.1.1 Background

In probabilistic risk assessments (PRAs) of nuclear power plants (or other technological systems), human reliability analyses (HRA) require considering a variety of factors, including the plant's state (e.g., the reactor's power level, reactor coolant system (RCS) pressure, temperature and level), the equipment being operated, tested, or maintained, and aspects of human-systems interfaces associated with the tasks being performed. Recently, there has been a growing recognition and concern that existing HRA methods do not represent realistically the roles of humans in both the initiation and the prevention (or mitigation) of accidents at nuclear power plants (NPPs). Examples of these concerns were presented by Dougherty and others in a special issue of Reliability Engineering & System Safety[1] (devoted to concerns about current HRA methods), Parry and Lydell,[2] and Wreathall and Reason.[3] Generally, these criticisms question the simplistic and narrow consideration of the factors that influence operators and other plant personnel, the limited consideration of the interactions between people and the plant, and the frequent assumption of independence between multiple unsafe human actions.

To understand the areas for development in HRA required to address these concerns, it is necessary to develop an explicit framework of the relationships between the disciplines of behavioral sciences, human factors, systems engineering, HRA and PRA. This development was propelled by, and is based on, a review of significant operational events described in an earlier report,[4] and the intention to make any new developments in HRAs to be as representative of real-world events as possible.

It is recognized that a framework that connects diverse disciplines including behavioral sciences, human factors, and systems engineering to HRA and PRA never will be totally complete. Consequently, the framework described in this report is not expected to be the "final" one; that described below has continued to evolve since the project's inception in early 1992. Some areas are identified for potential extension in later stages of the project. However, its purpose is essentially pragmatic. It is intended to help subsequent tasks develop and underpin their concepts by a unified set of common principles.

A.1.2 Previous Use of Frameworks

For the most part, with one principal exception, frameworks have been developed implicitly to describe how human errors should be represented in PRAs. For example, the first significant incorporation of human errors into a PRA was in the U.S. Nuclear Regulatory Commission's Reactor Safety Study (WASH-1400[5]) using the Technique for Human Error Rate Prediction (THERP).[6] This approach led to the incorporation of human-error events directly in the PRA logic models (primarily in the fault trees) in a structure similar to that used to incorporate the failures of individual equipment. This approach, with moderate changes, has been followed to this day. The changes that have been made are primarily in the representation of some errors (often, but not always, errors associated with misdiagnosis) in the event-tree models. While new methods for quantifying human errors have evolved since the Reactor Safety Study[5] to address specific types of errors, such as the Operator Action Tree (OAT) method[7] for misdiagnosis, and the Human Cognitive Reliability (HCR) method[8] for actions not taken in time, these have not clarified the relationship between the HRA modeling and its integration with the PRA process.

The one explicit framework, which was developed to describe the relationship between HRA and PRA, was the EPRI-sponsored Systematic Human Action Reliability Procedure (SHARP),[9] a procedure for combining the HRA tasks with the PRA activities. It specifies seven steps for incorporating human errors

into a PRA. For example, it identifies, different HRA modeling techniques that can be used to quantify different kinds of human errors incorporated in the PRA. However, it does not specify which performance shaping factors (PSFs) must be considered for human errors; that is left to the HRA technique selected by the analyst. In other words, SHARP is a flow model of the steps required for incorporating human errors into a PRA, not a framework that describes which PSFs must be taken into account within the HRA process itself. Subsequently, a variation of SHARP, called SHARP1, was developed for application specifically in the Individual Plant Examination (IPE)[22] program.

While the SHARP framework is useful for ensuring that HRA and PRA tasks are coordinated in a structured manner, it does not fulfill the requirements of this project to (1) describe the kinds of human errors that are potentially important to safety that are not considered in present HRA and PRA practices, and (2) identify the important influences on human performance found in significant operational events. These elements must be defined to allow the development of a new HRA method or methods.

To develop a framework that can support the evolution of a new HRA method, the relationships must be described between human actions and errors and the impact plant conditions and other influences have on them. Therefore, an important task of this project was to develop an HRA framework that defines and describes these relationships. This accomplishment also will provide a basis for later tasks to explore the issues associated with errors of commission (EOCs) and dependencies between multiple human actions, and to provide a foundation for considering ways to more realistically model and quantify human errors in PRAs.

A.1.3 Purpose of Report

The purpose of the report is to explain the development of an multidisciplinary HRA framework which describes the kinds of human actions potentially important to safety that are not considered presently in HRAs and PRAs and facilitates our understanding of the important influences on human performance found in significant operational events. In addition, the framework implications for future PRA modeling are described, as well as its use in human factors and other NRC programs.

A.2 DEVELOPMENT

The approach taken in this study is to develop a new HRA framework that is, to the extent practicable, an evolution from earlier HRA approaches. This choice was made deliberately, for several reasons. First, PRA modeling has been under development for about 20 years, with significant investments in areas like data analysis, hardware modeling, and sequence analysis. Consequently, it is advantageous for any new HRA methods to be consistent with these developments. In addition, it is unlikely that the broader community would accept new HRA methods that require substantially abandoning current approaches. Indeed, the need not to make fundamental changes in the PRA technology was one of the findings of the assessment of user's needs performed earlier in this project.[10]

Second, the current relationship between HRA and PRA has led to useful results. For example, many utility's PRAs have inferred the importance of human actions particularly in the recovery of potentially significant abnormal conditions. These results have been used to develop scenarios for simulator-based training, for example. In many cases, these results are the product of the qualitative evaluations, but some have come from the quantitative analyses (see, for example, the application of HRA results in BWR studies[11]).

Third, there is an established body of expertise in the HRA community. If a technology is developed that negates this expertise, then it is very unlikely to become an accepted method without compelling reasons from outside. Some approaches to developing new HRA technologies have fallen to this shortcoming because the benefits of their use were not readily apparent nor explicitly demonstrated within the community of intended users.

Finally, requiring a change to a completely new method is likely to have significant associated costs; these include direct costs, such as retraining analysts and acquiring of new computer codes. In addition, re-analysis of "old" studies may be required to identify "new" insights. None of these reasons is unique to HRA. A substantial change in any engineering discipline would have similar consequences.

A.2.1 Existing HRA Framework

Figure A.1 illustrates the relationship between HRA and PRA activities that was used implicitly in the Reactor Safety Study[5] and basically is that performed today. (As with any generality, there are a few exceptions).

The building blocks of the PRA model are the "basic events" that include different failure modes of components and subcomponents which, in combination, lead to failures of systems. The basic events are combined in the fault trees according to the definitions of system and functional failures. The combinations of fault trees are represented in the PRA event trees according to the plant state being analyzed (such as a loss-of-coolant-accident [LOCA] or other accident scenario) to describe combinations that lead to unacceptable accident conditions, such as core damage.

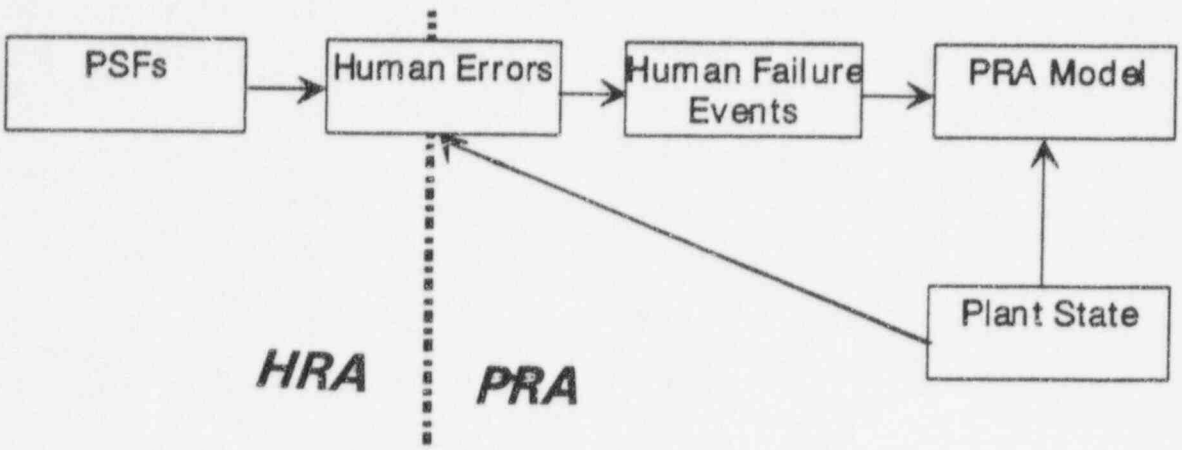


Figure A.1 Existing HRA/PRA framework

In this framework, human errors are incorporated into the PRA as a class of basic events, called human-failure events, that lead to system or functional failures, as in "operator fails to open recirculation suction valve" leading to failure of recirculation flow in a small-break LOCA.

These human-failure events are broadly undifferentiated, that is, no differences between various kinds of human actions are considered. For the most part, they are identified simply as "operator fails to _" or "maintenance technician fails to restore _." These identifications describe one failure mode of the associated pieces of equipment. For example, "maintenance technician fails to restore RHR pump 1A" describes a failure mode of the pump; it says nothing about the "human" aspects of the failure.

In many PRAs these events are evaluated on the basis of a small set of performance shaping factors (PSFs) which have included, for example, the timescale for actions, the effectiveness of annunciators, and the ability of a second person checking the first (see, for example, NUREG/CR-4550, Vol.1[12]). Other PRA studies have incorporated other PSFs, some more extensive, some subjectively developed. However, they have been applied frequently to large groupings of human error events with little consideration as to the specific kinds of errors these factors cause.

When human performance issues are analyzed, it is in the context of the accident scenario defined by the plant's state in the PRA. For example, the final HRA quantification is performed on a "cutset-by-cutset" basis, especially where the quantification of post-accident responses is based on the timescale available for action. Cutsets are the Boolean logic statements resulting from the event-tree models that define a unique combination of basic failure events that would cause the accident. One cutset may represent a combination of failures associated with a pump in one train and a valve in another train and failure of the operators to restore operation. The timescale available for operators to recover the valve close to the control room and prevent core damage in that cutset (i.e., the probability of recovery) may be quite different from a cutset that involved accessing some remote area of the plant. Hence, the influence of plant state on the human errors is not adequately nor appropriately accounted for in the PRA.

A.2.2 Refined Multidisciplinary HRA Framework

Figure A.2 presents the Refined Multidisciplinary HRA Framework. The most important changes lie in the explicit identification of different kinds of errors as possible causes of human failure events, and the addition of the role that plant conditions play in forcing human errors to occur. However, the first change is in terminology, i.e., denoting "human error" as a basic event.

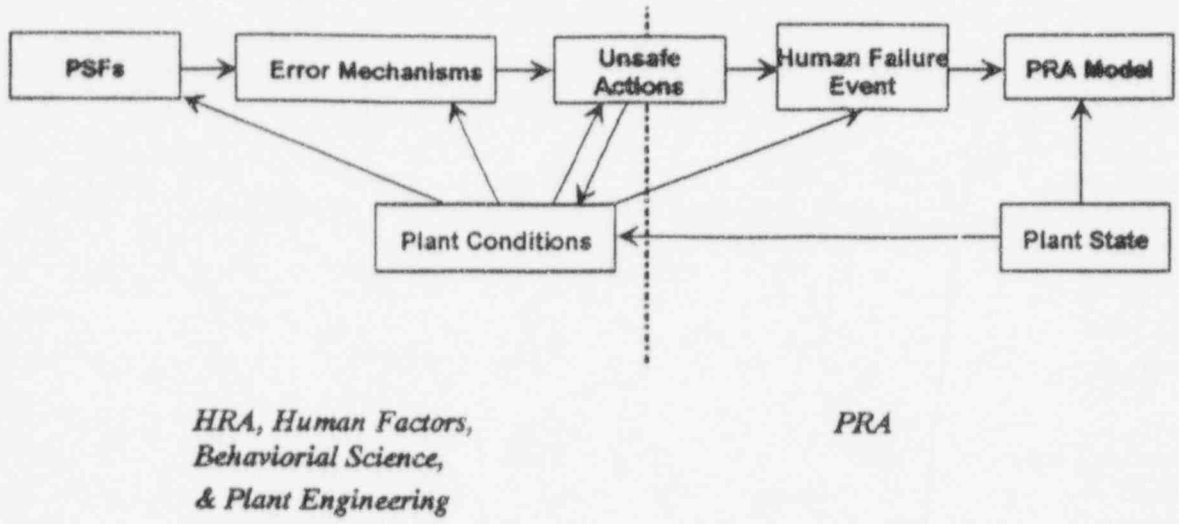


Figure A.2 Multidisciplinary HRA framework

A.2.2.1 Unsafe Actions Versus Human Errors

The term "human error" has been used by PRA analysts since the days of the Reactor Safety Study.[5] The term refers to a basic event in PRA involving a lack of action or an inappropriate action taken by the plant's staff that leads the plant to a less-safe state. However, the term "human error" when used by behavioral scientists often refers to quite different aspects in human behavior; more commonly, the issue of concern here is deficient cognitive processes. These meanings can be very different from those intended by the PRA analyst. In particular, the PRA concern is that an unsafe condition results; the reasons why the human error occurred generally are of limited importance. By contrast, from the perspective of the behavioral scientist, the consequence of the error generally is of limited interest compared with the causes underlying such an error.

For making the application explicit, the refined framework does not refer to human errors in relation to the PRA; instead, it refers to unsafe actions. Unsafe actions are those actions taken (or not taken when needed) by people that lead the plant into a less-safe state. Unsafe actions implies nothing about whether the action taken (or not taken) was a "human error", to avoid the inference of blame or that the human was the root cause of the problem. As described later, humans are often set up by circumstances and conditions to take the actions that were unsafe. In those circumstances, the people did not commit an error in the every-day sense of the term; they were doing what was the "correct" thing as it seemed at the time. One important aspect of unsafe actions is that they are observable by a witness; the person concerned either does something (or is observed not to do something). Here, the concern is only the actions taken in relation to the plant's safety.

Embedded in the definition of unsafe action is the requirement that the plant moves towards a less-safe state. However, the definition implies the question of how to judge safety, and when the plant is "in a less safe state?" Some aspects of safety are defined by the logic models in PRA; these systematically describe how safety is effected (in terms of barriers to the release of radioactive fuel from the vessel, the containment, and the site), principally by equipment operation or some operator's actions. However, a PRA does not presently provide a comprehensive definition of safety in itself. For example, the omission from PRAs of classes of human actions is the primary motivation behind this development program. In addition, simplifying bounding assumptions about a plant's behavior are required to make PRA studies feasible. Therefore, the judgment of whether the plant has moved from a more to a less-safe state requires judgments beyond those that could be resolved by present-day PRA models. In practice, while performing this project, such judgments have proved tractable. Within the nuclear-engineering community, there seems to be a broadly shared recognition of a plant moving towards a less-safe state, whether or not it would be explicitly included in a PRA. In practice, there have been no cases where uncertainty has remained about the direction of safety once all parties reviewed the event descriptions in detail.

As a result of the distinction between safety as observed in real-world NPP operational events and safety as represented by PRA modeling, not all unsafe actions correspond to human-failure events defined in PRAs. In some cases, there is a direct correspondence. For example, operators terminating operation of a needed engineered safety feature would be considered an unsafe action, and also should be incorporated as a basic human-failure event in the PRA. However, more commonly an unsafe action often does not correspond directly to a human-failure event. For example, in evaluating the 1992 loss of RHR at Prairie Island Unit 2, described later in this report, the unsafe actions were associated with draining the reactor coolant system (RCS) to midloop of the RCS hot legs (several feet above the top of the reactor core) in less than two days after reactor shutdown, while relying on indirect and temporary (tygon tube) indication of RV level. This led operators to fail to terminate draindown before RHR was lost. The observable unsafe actions were a miscalculation of the RCS's water level, and a miscalculation of the time to reach the target level. However, from the PRA perspective, the human-failure event would be an operator-induced, loss-of-coolant accident (LOCA) caused by draining down below midloop, with a consequential loss of all RHR for core cooling.

Recognizing the distinction between unsafe actions observed in event data and the errors of omission (EOOs) and errors of commission (EOCs) contained in the PRA-defined human-failure events, there also are important distinctions between classes of unsafe actions. These distinctions are important in terms of their likely impact on safety and risk, and on the factors surrounding their occurrence.

Figure A.3 summarizes the distinctions between the classes of unsafe actions, based on work by Reason.[13] Slips and lapses are unsafe actions where the outcome of the action was not what was intended. Skipping a step in a procedure or reversing the numbers in an identification label are examples of lapses and slips, respectively. Both are errors associated with what Rasmussen[14] has termed skill-based level of performance associated with the predominantly automatic control of routine, highly-practiced actions. The significance to risk of these unsafe actions seems to be quite small because, not being as intended, these actions are often easily recognized by the person involved and (in most circumstances) easily corrected. For example, HRA methods like THERP[6] primarily focus on slips and lapses.

There are two broad classes of unsafe actions where the action was performed as intended. The first relates to intentional actions in which the intention is wrong. For example, the operator may have misdiagnosed the plant's condition and is following the procedure for the wrong condition. These

consequential actions are mistakes. The second is 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, such as reversing the steps in a procedure to simplify it. Unsafe actions in this last category are circumventions. (It should be noted that acts of sabotage are distinct from circumventions in terms of the intended consequence, and are not within the scope of this project.) Each of these major categories have been subdivided as illustrated in Figure A.3.

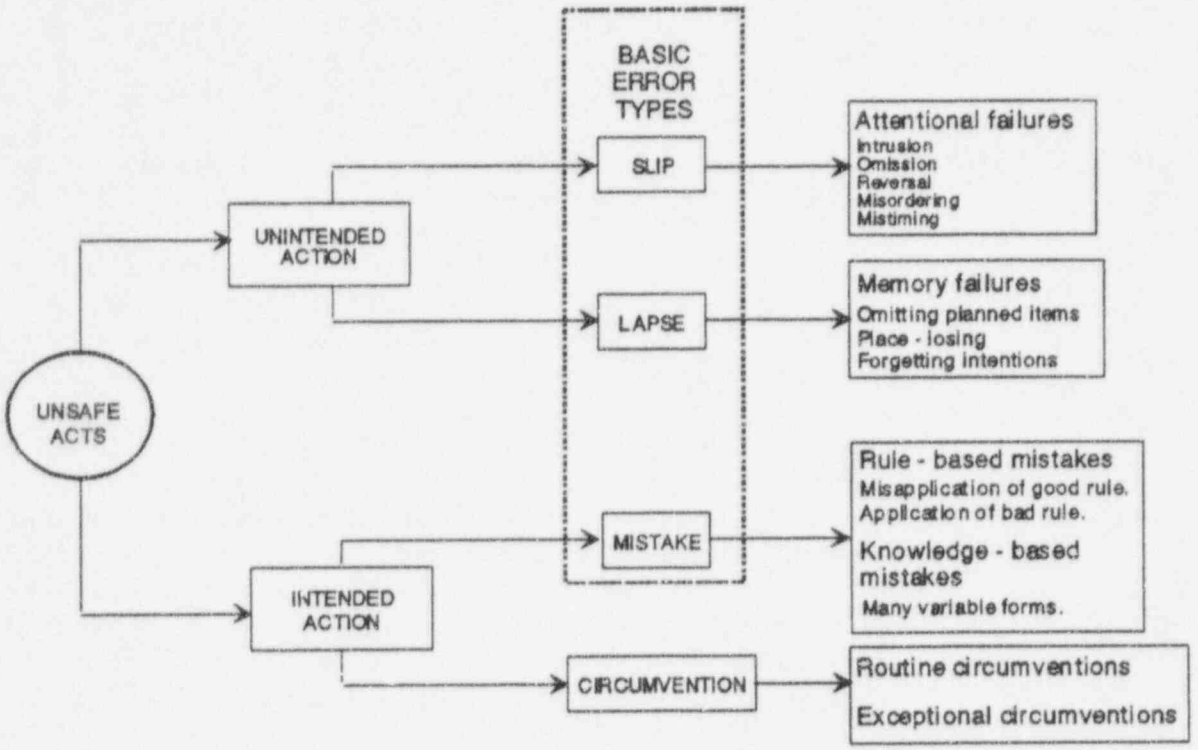


Figure A.3 Classification of unsafe actions

Mistakes can be considered rule-based (RB) or knowledge-based (KB) depending on whether the task demands rule-based or knowledge-based performance. For the former, documented task-specific instructions are being followed (usually contained in procedures for almost all power-plant activities important to safety). For knowledge-based performance, the person involved is relying on ingrained technical and specialist knowledge (as in generalized troubleshooting). Rule-based mistakes are further subdivided as to whether the wrong rules are being followed (e.g., following misdiagnosis), or the rules are appropriate but have technical omissions or flaws.

Mistakes are perhaps the most significant to risk because they are being followed purposefully by the user, who has limited cues that there is a problem. Indications contradicting the diagnosis are often dismissed as "instrument errors". Often, it takes an outsider to the situation to identify the nature of the problem, as happened in 1979 at Three Mile Island, Unit 2.

Circumventions are potentially significant contributors to risk in that unanalyzed conditions can result from unexpected combinations of errors and circumventions. However, two conditions seem to mitigate

this potential. First, the person committing the circumvention is aware (usually) that the action has occurred and can bring any significant consequence to the attention of other staff. However, attitudes towards punishment can influence this self-reporting heavily. Second, in the current environment in the nuclear industry, circumventions seem to be a rarely reported occurrence.

A.2.2.2 Error Mechanisms

Unsafe actions can come about from different psychological mechanisms. For example, an operator may fail to open a valve for several reasons. First, a step in a procedure requiring the valve to be opened may be skipped inadvertently. Second, the valve number in the procedure or on the valve control may be misread (for example, reversing two digits) and the wrong one opened. Third, the procedure being followed may have the step omitted from the task being performed. Fourth, the procedure may have been the wrong one. Fifth, the operator may perform the steps of the procedure out of their written sequence because it easier to do so, and consequently, fail to open the valve at the necessary time. From the PRA perspective, the unsafe action for all of these failures still is "operator fails to open valve."

These different reasons for failing to perform an action or performing another represent different error mechanisms. There are important differences between them, both in the conditions under which they can occur and as to the consequences, and ultimately, in their potential impact on risk.

Error mechanisms are not observable in themselves, only by their consequences as unsafe actions. Therefore, sources of data most commonly used, such as LERs, do not provide information specific to this classification. However, classification is important in that considering the error mechanisms provides a logical basis for considering the influence of PSFs and plant conditions on unsafe actions. The following discussion is primarily based on the discussion by Reason.[13]

Reason identified ranges of error mechanisms associated with different kinds of unsafe actions. For our purposes, these can be classified into two groups: failures associated with cognitive processes, and circumvention-related factors. Failures associated with cognitive processes (and their most likely-to-be-associated types of unsafe action) include the following:

- Failures in attention (mainly slips)
- Failures of memory (lapses)
- Failures of recognition (mainly lapses)
- Failures of situational appraisal (misapplications of a good rule [RB mistakes] and KB mistakes)
- Failures of verification (misapplications of good rule and KB mistakes)
- Motor program failures - applications of bad rule (RB mistakes)
- Incomplete knowledge (RB and KB mistakes)
- Inaccurate knowledge (RB and KB mistakes)

(We note that confirmation bias and overconfidence, for example, are subsumed under verification failures.)

A.2.2.3 Performance Shaping Factors

As depicted in Figure A.1 and A.2, performance shaping factors (PSFs) represent influences on both the occurrence, and type of human error mechanisms; for example, during operations, testing, and maintenance. Each error mechanism has a primary set of PSFs as summarized below. Given the

differences between the possible error mechanisms that could be the cause of one unsafe action, using a single set of PSFs for all mechanisms is inappropriate (except where one particular error mechanism is the most risk-significant).

- *Influences on attentional failures*: distraction, high workload, stress, changes in work routines, situations, or plans.

- *Influences on memory failures*: distraction, high workload, stress, and task items for which necessary knowledge must be kept in the head rather than being inherent in the task.

- *Influences on recognition failures*: poor "signal-to-noise ratio" (i.e., poor human-machine interface and communications), distraction, high workload, and stress.

- *Influences on situational appraisal failures:* counter-indications to applying the appropriate rule are embedded in a mass of other signals, some of which indicate the use of a "strong-but-wrong" rule, inadequate training, inadequate procedures, inadequate supervision, stress, and distractions.

- *Influences on verification failures:* as above, with greater emphasis on distraction, stress, workload, and other things likely to disturb or pre-empt on-line reasoning.

- *Influences on motor program failures:* a "forgiving" environment in which bad work habits are not corrected by supervision, experience, training, or adequate procedures.

- *Influences on knowledge failures:* inadequate procedures, training, and leadership.

These PSFs can be interpreted into the ergonomic and plant-behavior aspects of the human-system. The ergonomic aspects are termed the PSFs, and include such aspects as procedural format and content, training, and panel design. The PSFs used in this project are those identified using the Human Performance Investigation Protocol (HPIP)[4]. The plant-behavior aspects of the human-machine system are discussed below, under plant conditions.

The occurrence and location of circumventions is strongly influenced by the task's design and the occurrence of incompatible goals or requirements, and the rewards and penalties for compliance.

A.2.2.4 Plant Conditions

The final change in the framework is the addition of the plant conditions i.e., the specific features of the plant and its operating state that led not only to the task being performed, but also to the conditions under which it was performed. For 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 defined traditionally in the PRA, especially these that could lead to initiating events or other errors of commission (EOCs).

A detailed description of plant conditions is necessary to identify the possible situations in which people are almost forced into failure. For example, in the 1992 loss of RHR event at Prairie Island Unit 2,[15] the combination of workload, ambiguous task requirements or instructions, and a lack of supervision led

to an overdraining failure by operators who were draining the reactor coolant system (RCS) water level to midloop within 48 hours of shutdown. At this time, the decay-heat level was still sufficient to cause boiling in the reactor core approximately 20 minutes after the loss of RHR flow. This example indicates the level of specification for plant conditions that must be considered to define the conditions under which people can fail. In addition, this level of description allows the identification of EOCs since they primarily result from errors during periods of intervention with the plant (such as changing power levels, performing surveillance testing, or during low power and shutdown (LP&S) operations).

The distinction between PSFs and plant conditions is a pragmatic one since both influence the occurrences and types of unsafe actions. PSFs primarily are related to ergonomic aspects of the situation, which often can be evaluated by techniques such as walk-throughs and use of human-factors checklists. These types of PSFs primarily are latent deficiencies in the job-aids, displays, and training for a task that are revealed in the face of the unique characteristics of the plant and the activities being performed. The characteristics of the task are principally associated with the plant and its operating conditions which are often active and transient. In other words, the plant conditions are not observable until the task or evolution is underway, although with careful analysis, they may be foreseeable.

Plant conditions influence many of the other components of the framework: PSFs, error mechanisms, unsafe actions, and human-failure events; they are summarized as follows.

Influences of Plant Conditions on PSFs: Many PSFs depend on the plant conditions; for example, consider the differences between LP&S and at-power operations. Procedures for LP&S are different (and often less well proven). Instrumentation displays are different, such as RCS level being read from a plastic Tygon tube, rather than the installed RCS level-measurement system. Training is different, as in simulator-based training of operators for LP&S conditions very rarely being performed. Even under full-power operations, there can be differences between PSFs for different classes of accidents. Since plant conditions include the definition of plant state (i.e., as applicable to a PRA accident scenario), these aspects of plant conditions also must be considered as influences on PSFs.

Influences of Plant Conditions on Error Mechanisms: The plant conditions afford opportunities for errors and set the context for PSFs to play a significant influence in those opportunities. For instance, the plant conditions at the task level (e.g., maintaining a particular valve or draining the reactor water level to midloop within 48 hours after shutdown) provide specific opportunities for error mechanisms to arise. Maintaining the specific valve may require considerable attention to very fine details in the setup (as with a suction relief valve at one of the events reviewed). There, significant opportunities for errors associated with, for example, recognition or attentional failures were presented that would not be part of the maintenance of other mechanically simpler valves. Similarly, during that valve-maintenance task, deficiencies in PSFs like lighting, clarity of procedures, and so on, become important in influencing the probabilities of error mechanisms. That is, plant conditions determine the sensitivity of error rates to the PSFs and provide the opportunities for error mechanisms to become manifest.

Interactions of Plant Conditions With Unsafe Actions: Plant conditions provide the setting in which the occurrence of an error mechanism results in a specific unsafe action. Using a simplified example to illustrate this, consider a failure in attention that results in skipping a step in a procedure; the consequential unsafe action that results depends on the instructions that were skipped. If they were associated with plant conditions requiring operators to perform some time-critical recovery action in a post-accident phase, the unsafe action would be the failure to start the components listed in the procedure. This would be considered in a human-failure event modeled in the PRA as having the potential of

contributing to the frequency of core damage. However, if the step omitted was to reconfirm a previously identified alarm condition the same error mechanism will have no direct unsafe consequences and would also not be considered in the PRA human failure event. In other words, the same error mechanism may lead to very different unsafe actions depending on the plant conditions.

In addition, the unsafe actions themselves change the plant conditions. For example, a mistaken intervention, such as terminating the operation of an engineered safety feature, creates a new plant condition in which, for example, the removal of decay heat from the core is no longer in effect. The unsafe intervention can create new conditions that require new actions by operators, possible on different time scales, compared with the case if no action had been taken. In this way, cycles of human interventions (both beneficial and detrimental) can require consideration on a cycle-by-cycle basis as far as creating new plant conditions are concerned. They also can create the opportunity for a new set of PSFs and error mechanisms to initiate additional unsafe actions.

There are two forms of interactions of unsafe actions with plant conditions: *unsafe actions of omission and unsafe actions of commission*. Unsafe actions of omission (UAOs) are where people fail to take an action or series of actions that would put the plant in a safer state, or at least prevent its continued deterioration. Unsafe actions of commission (UACs) are those interventions taken by people that place the plant in a less safe condition. We note that these UAOs and UACs do not necessarily correspond with the PRA-defined human-failure events of errors of omission (EOOs) or errors of commission (EOCs) in the same way that unsafe actions may (in general, as described in Section B.2.2.1), but do not necessarily, correspond to human-failure events in the PRA context.

Influences of Plant Conditions on Human-failure Events: Plant conditions (partly as an extension of the PRA-defined plant state) set the context for the consequences of the unsafe action in terms of the impact on plant systems. For instance, omitting a step from a procedure can result in failure to start equipment as described above; this would be an error of omission. However, omitting a step in a procedure that gave cautions that the following step was only to be performed under certain conditions, could result in the inappropriate performance of the next step; this inappropriate action would be an EOC. Consequently, the distinction between EOOs and EOCs can be almost entirely set by the plant conditions, although the same unsafe action (omitting a step in a procedure) is involved.

A.2.3 Potential Additions

Any framework is an aid to further developments, and, as such, it can never be considered complete. Therefore, the need for potential changes and additions must be recognized at all stages in the project. Hence, the following are recognized as having a potential for addition and integration in the future.

A.2.3.1 Organizational Influences

Figure A.4 indicates the potential for incorporating organizational influences as a set of potential influences. The most obvious ones are programmatic influences on the PSFs, such as training and procedures programs. The University of California, Los Angeles (UCLA) is developing such an approach.[16] Organizational influences have the potential to act on all such programmatic activities through such influences as budgeting or allocation of other resources, goal-setting, communications, and work formalization. The mechanisms by which programmatic influences act have been reviewed, for example, by Olson, et al,[17] Wreathall, et al.,[18] and Haber, et al.[19]

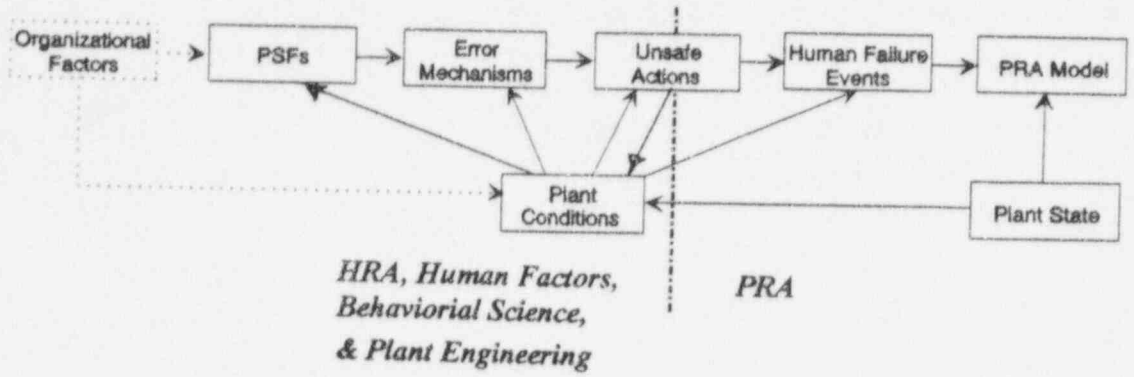


Figure A.4 Incorporation of organizational influences within framework

In addition, organizational factors potentially can influence the plant conditions. For example, a situation arose where a plant drained water from the reactor coolant system (RCS) in preparation for midloop operations in less than two days after shutdown. At this point, there was significant decay heat in the reactor core (a plant condition), yet no preparations were made to provide a measure of additional protection as often done when decay heat levels are much lower. (This event is discussed in more detail in Section A.3.1.)

While it is recognized that organizational factors have the potential to be significant influences, they are not represented explicitly in the framework as yet. Their inclusion is projected in Figure A.4, but until more structure is provided for their effects, it is considered as an area for future incorporation.

A.2.3.2 Sub-classification of performance-shaping factors

Others have subdivided PSFs into various groupings. For example, Swain and Guttmann[6] considered external PSFs and internal PSFs. External are those PSFs related to procedures, training, human-system interface, and so on, which are the products of plant programs controlled by organizational processes. Internal PSFs are those more related to individuals, such as stress, technical knowledge, and so on. To some degree, the internal PSFs are influenced by plant programs (e.g., selection of personnel) but much less directly than the external PSFs (e.g., procedures). If the organizational influences are added to the framework, as discussed in Section A.2.3.1, then the PSFs should subdivided into those strongly influenced by organizational influences (external PSFs) and those that are not (internal PSFs). The organizational influences then can be described more completely.

A.2.3.3 Evaluation of Successful Event Data

So far, the framework has concentrated on events involving failures in human performance, partly because such events are more often identified explicitly in reports, and because PRA models are principally expressed in terms of failures. However, for reasons discussed earlier in relation to plant conditions, many instances can occur when failures do not result, even though the circumstances are challenging. While such successes may not change the substance of the framework, their analysis may

draw more sharply the effects of plant conditions on causing or shaping the effects of error mechanisms. For example, additional analyses of events could be created around instances of:

- Successful recovery because of "..." and
- Successful recovery in spite of "...".

The factors following the "..."s would be plant conditions, PSFs, and, perhaps, organizational factors.

A.3 EVALUATION OF FRAMEWORK IN ANALYSIS OF EVENTS

This section describes how the framework can bring structure to a description of human performance in a significant operational event, and to provide a basis for evaluating quantitatively data derived from event reports.

A.3.1 Evaluation of a Significant Operational Event

The following event description indicates, by example, how the concepts described in the framework can be used to bring structure to the analysis of human performance during a significant operational event.

The event in question is the 1992 loss of RCS inventory and loss of RHR at Prairie Island Unit 2 on February 1992 and was the subject of a Regional Augmented Inspection Team (AIT) report.[20] Table A.1, taken from NUREG/CR-6093,[4] identifies the essential elements of the event. Figure A.5 is a representation of the event according to the Multidisciplinary HRA Framework. In the event, operators were reducing the RCS inventory to reach midloop conditions (one of the possible operating states during a refueling outage) by the second day after the reactor was shut down. The reactor decay-heat level was still approximately 6 MW. As is common practice at other reactors, the reactor water level was being measured by a temporary level-measurement system (using a Tygon tube) because the permanent level instrumentation was not compatible with the plant conditions (use of nitrogen overpressurization). Using this temporary instrumentation required the operators to calculate the water level taking into account of the effects of the nitrogen overpressurization. In addition, the operators used the calculated draindown rate to estimate the time when the targeted midloop level would be reached. Because of a combination of several calculational errors and poor communication between the operating crew and their supervisors, the RCS level was reduced to the extent that suction pressure to the pump used for core cooling (one RHR pump) was lost, the pump became airbound, and core cooling was lost for 21 minutes. Because of the level of decay heat and the loss of forced cooling, boiling took place in the reactor. In addition, the containment was open, with temporary cables passing through open penetrations and the mechanical interlocks on the personnel access door disabled. From this event, the following observations can be made with reference to the refined Multidisciplinary HRA Framework described in Section A.2.

First, the human-failure event was overdraining the RCS causing a loss of RHR; this would be a LOCA initiating event in a low-power and shutdown (LP&S) PRA. This classification indicates that recovery of core cooling involves more than simply restoring operation of the RHR pump; refilling the RCS is a prerequisite before restoring of core cooling by RHR, which has an impact in the recovery analysis.

This human-failure event resulted from two unsafe actions: miscalculation of the RCS water level, and miscalculation of the time to reach the target level (only partly influenced by the first miscalculation). In part, these were influenced by a lack of communications with operations supervisors who could have detected these errors, based on their experience during previous similar operations.

Both unsafe actions were rule-based mistakes. The procedures gave no direct guidance on the accuracy required in the calculations, important parameters were not provided, and checkpoints were not included that could have led to the discovery of the incorrect RCS level calculations. These procedures were applied by the operators as written.

Table A.1 Summary of 1992 Prairie Island Unit 2 Loss of RHR Event

Event: Loss of RHR for 21 minutes

Situation	Acts	Defenses	Conditions	Influences
1. Day 2 of outage; decay heat is high (approximately 6 MW). In-vessel boiling occurred. 2. Installed permanent level instrumentation not compatible with planned evolution (N_2 gas overpressure). 3. Temporary level instrumentation required accurate manual calculations. 4. Both permanent and temporary redundant instrumentation relied on single common pressure-measurement sensor. 5. Small errors in estimated timescale for drain to midloop led to unacceptable plant conditions (airbinding of cooling pumps).	1. Two rounding errors made by operators in calculating RCS level. 2. Operators over-reduce RCS level, which causes vortez (this is based on Shift Manager's faulty calculation of drain-down time). RHR pump fails due to airbinding. 3. Little discussion with shift operations management about problems during event.	1. Multiple RCS refill routes available. *+Design* 2. Operators trip RHR pump on early evidence of airbinding. *+Training* 3. Once RHR pump was tripped, AOP and EOP led operators to successful recovery. *+Procedures* 4. Containment evacuated according to procedure. *+Procedures*	1. Two related procedures (RCS level and draindown time) required extensive, detailed calculations with no aids provided. *-Human Engineering* 2. Temporary RCS level instrumentation very difficult to read in poor environment. *-Human Engineering* 3. Operating personnel had limited or no training in draindown tasks. Experienced personnel allocated to other parallel tasks. *-Training, Supervision* 4. Draindown procedure not clear on prerequisites for instrumentation availability. *-Procedures* No communication with shift operations management led to lost opportunities to correct errors in level control. *-Communications* 5. No communications from plant personnel, who heard pump "burping," led to delay in identifying impending airbinding. *-Communications*	Procedures: -1; +2 Training: -1; +1 Communications: -2 Human Engineering: -2 Supervision: -1 Design: +1

Source: AIT Report 50-306/92-005.

---

* + indicates a positive defense, condition, or influence in the event
  - indicates a negative defense, condition, or influence in the event

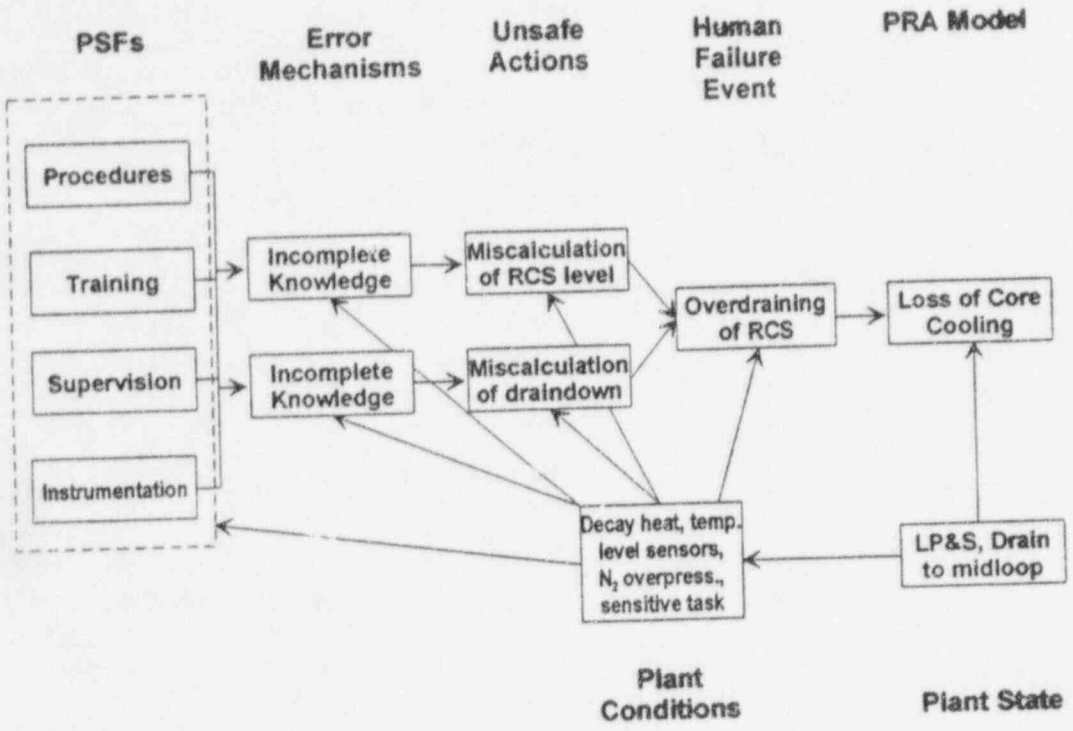


Figure A.5 Representation of 1992 Prairie Island Unit 2 loss of RHR event in multidisciplinary HRA framework

The PSFs for these two mistakes were primarily the inadequacies in the procedures (summarized above). In addition, the operators making the calculations had not been trained in the procedure and had not performed the task before. A lack of supervision allowed the errors to continue. Of somewhat peripheral importance to this event was the difficulty in reading the indicated level on the temporary instrumentation.

Of considerable importance in this event were the plant conditions. First was the high decay-heat level that created the hazard whereby the core could be put at risk by a relatively brief loss of cooling. Second was the inoperability of the installed RCS level instrumentation, a result of the design of the electronic RCS-level measurement system that was rendered offscale by the nitrogen overpressure with the computer-based display system indicating a "failed" status. Third was the sensitivity of the task to small errors in the calculations, such as rounding off of numbers and discrepancies between sources describing the cross-sectional areas of tanks. Figure A.5 illustrates these relationships.

A.3.2 Quantitative Evaluation of Human Actions in HACS Database

The following analyses were made to test the concept of the framework against data in the Human Action Classification Scheme (HACS) database and to illustrate how the framework could be used to develop information about human performance. These data were analyzed and interpreted at an interim stage of the HACS database development. Later tasks (particularly Tasks 7 and 8 - see Appendix B and C)

involved separate analyses of more recent versions of the HACS database. Any inconsistencies between the following data and those contained in subsequent reports should be considered in this context.

Further, it is recognized that the database contains comparatively few events where there were sufficient data to classify the unsafe actions and PSFs specifically. These were the PWR LP&S events analyzed using full-text licensee event reports (LERs). Therefore, these results do not represent resilient statistics;. rather, they are intended to portray the kinds of information that could be extracted from databases using the analytical structure of the framework.

The data presented in the following tables represent results only for those events where the database showed a datapoint; in those cases where there was a blank entry (e.g., the type of error was not identified), the event was discarded to avoid skewing the results. Tables A.2 through A.5 show the results of analyses for events that were initiated by unsafe human actions. Table A.2 indicates that rule-based mistakes ("RB mistakes") and slips were the most common kinds of errors for various initiating event types. Slips most often were associated with loss of offsite power (often the accidental contact of wires or knocking of relays) and were an equivalent contributor with rule-based mistakes in events involving loss of RHR. Knowledge-based mistakes ("KB mistakes") were reported for only one event - a loss of RHR event. Table A.3 indicates that UACs were more frequently attributed to an event initiator than UAOs. Table A.4 further identifies that these UACs were predominately the result of either a slip, or a rule-based mistake. Table A.5 shows that there is a differentiation between the PSFs associated with RB mistakes and slips. Communications, procedures ("situation not covered"), and supervision are associated primarily with RB mistakes, while design and training ("situation not covered") were more strongly associated with slips.

Table A.2 Number of Event-Initiator Unsafe Actions by Error Type for Initiating Event Type

Error Type→ / Initiating Event Type↓	Knowledge-Based Mistakes	Rule Based Mistakes	Slips
ESF Initiation	0	1	1
Loss of offsite power	0	3	5
RCS draindown	0	2	0
Loss of RHR	1	4	4

Table A.3 Number of Event-Initiator Unsafe Actions of Commission (UACs) and Omission (UAOs) by Initiating Event Type

Error Mode→ / Initiating Event Type↓	UAC	UAO
ESF Initiation	2	0
Loss of offsite power	7	1
RCS draindown	2	1
Loss of RHR	7	2

Table A.4 Number of Event-Initiator Unsafe Actions of Commission (UACs) and Omission (UAOs) by Error Type

Error Type→ / Error Mode↓	Knowledge-Based Mistakes	Rule-Based Mistakes	Slips
UAC	1	9	8
UAO	0	1	2

Table A.5 Number of Event-Initiator Unsafe Actions Associated with Error Type by PSF Type

Error Type→ / PSF Type↓	KB Mistakes	RB Mistakes	Slips
Communications	0	4	1
Design	0	0	2
HMI (Alertness)	0	0	1
HMI (Displays)	1	2	1
HMI (Labels)	0	1	0
Procedures (Layout)	0	1	2
Procedures (Not used)	0	1	1
Procedures (Sit.not covered)	0	6	4
Stress	1	0	0
Supervision	0	2	0
Training (Inadequate Instruction)	0	2	3
Training (Sit.not covered)	1	0	2
Work Environment	0	0	1
Other	0	0	1

Tables A.6 through A.10 display the results for other human-failure events, i.e., unsafe actions that were not associated with the event initiator. All the unsafe actions in this category were latent errors that rendered the event more complex or played a role before the initiating event, and were primarily rule-based mistakes (Table A.6). Tables A.7 and A.8 show that the most frequent activity associated with causing these non-initiator failure events was operations, especially in the case of loss of RHR; slightly more frequently, these events were the result of unsafe actions of commission (UACs). Table A.9 lists the PSFs identified for these unsafe actions; again, rule-based mistakes predominantly were influenced by procedures (all categories), and training. Because of the small number of slips (3), their PSF data is very sparse.

Table A.6 Number of Non-Initiator Unsafe Actions by Error Type for Event Type

Error Type→ / Event Type↓	RB Mistake	KB Mistake	Slips
ESF Initiation	1	0	0
Loss of offsite power	1	0	0
RCS draindown	2	0	1
Loss of RHR	7	0	2

Table A.7 Number of Non-Initiator Unsafe Actions by Activity for Event Type

Activity→ / Event Type↓	Design	Maintenance	Testing	Operations
ESF Initiation	0	0	0	1
Loss of offsite power	0	0	1	0
RCS draindown	0	1	1	1
Loss of RHR	2	2	1	4

Table A.8 Number of Non-Initiator UACs and UAOs by Event Type

Error Modes→ / Event Type↓	UACs	UAOs
ESF Initiation	0	1
Loss of offsite power	0	1
RCS draindown	2	1
Loss of RHR	6	3

Table A.9 Number of Non-Initiator Unsafe Actions by Error Type for PSF Type

Number of UAs→ / PSF Type↓	KB Mistakes	RB Mistakes	Slips
Communications	0	1	0
Design	0	3	1
HMI (Alertness)	0	0	0
HMI (Displays)	0	2	1
HMI (Labels)	0	1	0
Procedures (Layout)	0	4	2
Procedures (Not used)	0	1	0
Procedures (Situation not covered)	0	2	0
Stress	0	0	0
Supervision	0	0	0
Training (Instruction LTA)	0	2	0
Training (Situation not covered)	0	0	0
Work Environment	0	1	1
Other	0	1	0

Tables A.10 through A.14 show the results for recovery actions. Table A.10 identifies that most recovery actions were the result of rule-based behaviors (8 actions - usually while following procedures), with only two cases of knowledge-base behavior. Most loss of RHR events and slightly more loss of offsite power events were recovered outside the control room (Table A.11). Tables A.12 and A.13 indicate that the average and maximum recovery times for all categories except loss of RHR were longer for in-control room recoveries than for those outside the control room. In addition, recovery of RHR outside the control room often involved venting which required the longest recovery time. Where reported, most recovery actions were directed by of licensed operators (Table A.14).

Table A.10 Number of Recovery Actions Associated with Rule-Based or Knowledge-Based Behaviors by Event Type

Behavior Type→ / Event Type↓	Rule-Based Behaviors	Knowledge-Based Behaviors
ESF Initiation	0	1
RCS draindown	2	0
Loss of RHR	6	1

Table A.11 Number of Recovery Actions by Primary Location for Event Type

Location→ / Event Type↓	In Control Room	Outside Control Room
ESF Initiation	1	0
Loss of offsite power	2	3
RCS draindown	3	1
Loss of RHR	7	10

Table A.12 Average Recovery Times Associated with Primary Location for Event Type

Location→ / Event Type↓	In Control Room	Outside Control Room
ESF Initiation	16 min	-
Loss of offsite power	65 min	33 min
RCS draindown	158 min	83 min
Loss of RHR	31 min	59 min

Table A.13 Maximum Recovery Times Associated with Primary Location for Event Type

Location→ / Event Type↓	In Control Room	Outside Control Room
ESF Initiation	16 min	-
Loss of offsite power	65 min	59 min
RCS draindown	190 min	83 min
Loss of RHR	88 min	241 min

Table A.14 Number of Recovery Actions Associated with Primary Personnel Type for Event Type

Personnel Type→ / Event Type↓	Licensed Operators	Non-licensed Operators	Maintenance Technicians
Loss of offsite power	3	1	1
RCS draindown	4	0	0
Loss of RHR	12	4	1

The occurrence of multiple unsafe actions played a role in most event types; Table A.15 indicates that these were most common with loss-of-offsite-power events and RCS draindown events. Table A.16 indicates a somewhat subjective summary in which PSFs appeared to have a more significant influence (i.e., in terms of frequency) on unsafe actions that are either rule-based mistakes or slips, based on a compilation of their appearance in the different unsafe action categories (i.e., event initiator and non-initiator unsafe actions), as identified in Tables A.5 and A.9. The designation of an H, M, or L, indicate a high, medium, or low level of PSF significance, respectively.

Table A.15 Number of Events Involving No, One, or Two Unsafe Actions (UAs) by Event Type

Number of UAs→ / Event Type↓	No UA*	One UA	Two UAs
ESF Initiation	0	3	0
Loss of offsite power	0	5	3
RCS draindown	1	4	3
Loss of RHR	0	12	2
* - recovery only			

Table A.16 Composite Evaluation of PSF Significance Level for Error Type*

Error Type→ / PSF Type↓	RB Mistakes	Slips
Communications	H	L
Design	M	M
HMI (Displays)	H	M
HMI (Labels)	M	L
Procedures (Layout)	H	H
Procedures (Not used)	M	M
Procedures (Situation not covered)	H	H
Stress	L	L
Supervision	M	L
Training (Instruction LTA)	H	M
Training (Situation not covered)	M	M
Work Environment	L	M

* KB Mistakes not included

A.4 CONCLUSIONS & POTENTIAL USES OF FRAMEWORK

A.4.1 Conclusions

The framework provides a structure that relates the disciplines of human factors, human reliability analysis, and probabilistic risk assessment explicitly into single focused activity. It was found to enrich the qualitative analysis of operational events, particularly by focusing on the interaction between human performance and plant conditions that results in significant events. This enhancement shows that programs aimed at only one of the factors will never be entirely successful because it is their interplay that causes the significant events.

In addition, the framework can be used as a basis for analyzing event reports and deriving data. While the data quoted in this report are too sparse to form a statistically significant basis for HRAs and PRAs, the structure can applied to additional events, which could give useful statistics.

One hypothesis of the cause of major accidents - operating outside designer's expectations, thereby entering a regime where the plant's behavior is not understood (usually, an unforgiving condition), followed by failure to believe accumulating evidence - appears to be supported by the framework and events analyzed by using it as a basis. This breakdown is not reflected as such in PRAs. Without it, PRA is only a partial reflection of the causes of risk.

This framework continues to evolve; at least three possible additions were identified in Section A.2.3. It is expected that as knowledge in the behavioral sciences develops, as more events are reviewed, and as subsequent tasks are performed, the framework will change. Its capability for adapting and expanding is seen as an important feature. No findings from actual events should be discarded simply because they do not fit the framework model. No area relevant to human performance in NPP activities should be excluded because it is not considered within the framework scope. On the other hand, components are included only when they are potentially important to NPP safety.

A.4.2 Potential Uses of Framework

The framework provides a basis for describing the relationships among behavioral science, HRA, and PRA - a framework that can shape further analysis of operational data, guide HRA modeling, and integrate quantitative HRA and PRA. In the following sections, the use of the framework in a variety of applications beyond this project is discussed.

A.4.2.1 Use of Framework in PRAs

Can the framework improve the state-of-the-art in PRA? A few specific examples clarify that it can.

- **Theoretical Foundation.** The framework provides a more rigorous theoretical foundation for modeling and quantifying human reliability than has been available previously. HRA methods commonly used in PRAs are based on expert opinion or artificial test data. By establishing an investigational structure for returning to the actual operating experience, key aspects affecting human error can be analyzed. By clarifying the language and relating the concepts in the different disciplines of psychology, human-factors engineering, HRA, and PRA, these disciplines can be joined in synthesis rather than ignoring each other.

The benefits of such a framework as this is described in the NRC's own assessment of the state of PRA, presented in NUREG-1050.[21] The section discussing the state-of-the-art in HRA (A.3) stresses the need for an expanded understanding of human-system interactions. That assessment concludes: "However, 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." The framework presents the basis for this strengthening. Subsequent tasks in this project will develop the tools to finish this job.

- **Character of Serious Accidents**. This and related work suggests that there are common factors in the most notable events which have occurred in nuclear power history (i.e., Chernobyl, TMI) that also are common to the events (particularly LP&S) analyzed for this project. These are the common characteristics of serious accidents:

  - The plant is operated outside the designer's intentions;
  - The plant then enters a regime where plant behavior is not understood; and,
  - Operators refuse to believe accumulating evidence.

Recent discussions with analysts of transportation and aviation accidents believe that these factors generally are present in most serious accidents involving human operational control. Moreover, these three aspects are not modeled well (or even at all) in existing PRAs. While never stated succinctly, this observation may be part of the uncomfortable feeling expressed by many that human error is a dominant contributor to risk, and that instrumentation likewise must be important to risk, even if PRAs do not show this.

This framework and review of operating events focus directly on these three conditions that are involved in most serious accidents. This program will define how to model and quantify the related human responses, opening an area of major importance to the risk management structure of PRA.

- **Quality Improvement & Completeness.** A PRA can be only as complete as the accumulated knowledge of the analysis community. For PRAs to remain the best source of information on plant safety and risk, continuing review of operating events is essential. The framework provides a mechanism to identify new information, "surprises" if you will, from precursor events that then can be used to revise existing PRAs, improving their accuracy.

- **Dependency**. Dependency was identified as a major factor among human actions following an accident. The framework can ensure that the important aspects of human dependency, errors of commission (EOCs), and circumventions are included in PRA models. This capability will be taken up in subsequent tasks.

A.4.2.2 Use of Framework in Human Factors Studies

Although the framework was developed to support the use of HRA in PRA, it has become clear that it also can impact efforts in other areas. Perhaps equally important is the field of human factors. The following are examples of areas where this framework may provide an important contribution in NPP safety:

- **Development of New Human Factors Guidelines.** Given the integration of human performance and plant conditions, the framework can provide a basis for new ways of assessing, human-system interfaces, procedure-development programs, and training. For example, it may be possible to train operators to recognize and react intelligently when the bulk of the accumulating evidence is counter to expectations. Such guidelines should include paying special attention to the conditions under which errors are more risk-significant. In addition, many significant events involve actions outside the control room yet these have limited guidelines on human-factors issues.

- **Selection of Training Scenarios**. While the nuclear industry has made great strides in the selecting more realistic scenarios for operator training programs, many plant conditions are implicit in these scenarios, such as the plant is within technical specifications limits. Based on the review of significant operating events, the more challenging situations often involve conditions that are outside of the assumptions implicit in the training program. A continuing review of operational events using the framework would indicate what additional kinds of scenarios should be considered for training.

- **Development of Tools for "High-Risk" Scenario Management.** With additional event analyses (including consideration of the successful events discussed in Section A.2.3.3), it should be possible to clarify the modeling of plant conditions to specify under what conditions operations are "high risk." In such cases, where the consequences of human errors are great, additional human-factors reviews could be performed or additional aids provided to extend the scope of the plant's defenses. These would be limited only to high-risk scenarios because the methods would be expected to be labor- and resource-intensive. In practice, few analyses could be expected, and therefore, they must be focused on important scenarios.

A.4.2.3 Use of Framework in NRC Programs

Finally, the framework with its new perspective may be applied to NRC programs to expand their effectiveness.

- **Evaluation of Advanced Reactor Designs**. The roles of plant personnel in the operating of the advanced reactor designs will be different from those in current light-water reactors. There will be a greater emphasis on the use of passive plant features and automation, and less on post-accident recovery actions. The contribution of humans to risk in these designs has been claimed to be reduced, but this is based on existing methods of analysis; no systematic examination of the human contributions to risk for the new plants has been published. Such an examination should identify all the pathways that human errors could contribute to risk, including those involving departures from planned operating conditions. As discussed earlier, these departures are rarely random but are a product of plant conditions, which can be evaluated.

- **Accident Sequence Precursor Program.** The scope of this program could be expanded to identify the precursors to real, serious accidents in terms of the framework. Only limited scope HRA models are used, and they do not correspond to the issues identified in the framework. The current approach focuses only on hardware-vulnerable plant conditions the usually are recoverable if the operators are on track.

- **Onsite Inspections**. Personnel performing onsite inspections could be taught to apply the framework in the review of actual events. For example, they could be trained to be wary of proposed operations that can take the plant into uncharted waters. Also, it could help them understand that circumventions

are sometimes necessary, but can lead to unexpected conditions. They should be educated to demand careful plant planning and require briefings when challenges to plant boundaries are proposed (such as during LP&S conditions) and there is limited availability of instrumentation.

A.5 REFERENCES

1. *Reliability Engineering & System Safety*, Special Issue on Human Reliability Analysis, Vol. 29, No. 3, pp. 281-410, Elsevier Science Publishers Ltd: England, United Kingdom, 1990.

2. Parry, G.W., and Lydell, B.O.Y., HRA and the Modeling of Human Interactions, in *Probabilistic Safety Assessment and Management*, (Ed: G. Apostolakis), Elsevier Science Publishers Ltd: England, United Kingdom, 1990.

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

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

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

6. Swain, A.D., and Guttmann, H.E., *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, Sandia National Laboratories: Albuquerque, NM, August 1983.

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

8. Hannaman, G W., Spurgin, A.J., & Lukic, Y.D., A Model for Assessing Human Cognitive Reliability in PRA Studies, in *Proceedings of the 1985 IEEE Third Conference on Human Factors and Power Plants, Monterey, California*, Institute of Electrical and Electronics Engineers: New York, NY, 1985.

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

10. Haas, P.M., Bley., D.C., and Whitehead, D.W., *Integrated HRA Methodology User Needs Assessment* (Draft Letter Report), Sandia National Laboratories: Albuquerque, NM, August 1993.

11. Andersen, V.M., and Burns, E.T., Human Error Probability Models in the BWR Individual Plant Evaluation Methodology, *Proceedings of the 1988 IEEE Fourth Conference on Human Factors and Power Plants, June 5-9, 1988, Monterey, California*, Institute of Electrical and Electronic Engineering: New York, NY, 1988.

12. Ericson, D.M., et al, *Analysis of Core Damage Frequency: Internal Events Methodology*, NUREG/CR-4550, Vol. 1, Rev. 1, Albuquerque, NM: Sandia National Laboratories, 1990.

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

14. See, for example, Rasmussen, J., Models of Mental Strategies in Process Plant Diagnosis, in *Human Detection and Diagnosis of System Failures*, (J. Rasmussen & W. Rouse, Eds.), New York: Plenum Press, 1981.

15. Steinke, W., Hill, S., Meyer, O. and Kauffman, J., *Trip Report: Onsite Analysis of the Human Factors of an Event at Prairie Island 2, February 20, 1992, Loss of Shutdown Cooling*, EGG-HFRU-10228, Idaho National Engineering Laboratory: Idaho Falls, ID, April 1992.

16. Davoudian, K., Wu, J. S., & Apostolakis, G., Incorporating Organizational Factors into Risk Assessment Through the Analysis of Work Processes, To be published in *Reliability Engineering and System Safety*, Elsevier Science Publishers Ltd: England, United Kingdom, (Draft) 1993.

17. Olson, J., Chockie, A.D., Geisendorfer, C.L., Vallario, R.W., and Mullen, M.F., *Development of Programmatic Performance Indicators*, NUREG/CR-5241, Battelle Human Affairs Research Centers: Seattle, WA, 1988.

18. Wreathall, J., Schurman, D.L., and Anderson, N.A., An Observation on Human Performance and Safety: The Onion Model of Human Performance Influence Factors, in *Probabilistic Safety Assessment and Management*, Elsevier Science Publishers Ltd: England, United Kingdom, 1991.

19. Haber, S.B., O'Brien, J.N., Metlay, D.S., and Crouch (Shurberg), D.A., *Influence of Organizational Factors on Performance Reliability*, NUREG/CR-5538, Brookhaven National Laboratory: Upton, NY, 1991.

20. *Augmented Inspection Team Report: Prairie Island Unit 2 Loss of Decay Heat Removal, February 20, 1992*, AIT Report 50-306/92005, U.S. Nuclear Regulatory Commission, Region III: Glen Ellen, IL, 1992.

21. *Probabilistic Risk Assessment (PRA) Reference Document*, NUREG-1050, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research: Washington, DC, 1984.

22. *Individual Plant Examination (IPE) for Severe Accident Vulnerabilities - 10 CFR 50.54 (f)* (Generic Letter No. 88-20), U.S. Nuclear Regulatory Commission: Washington, DC, 1988.

APPENDIX B

IDENTIFICATION AND REPRESENTATION OF ERRORS OF COMMISSION (EOCs)

(FIN L-2415, Task 7)

S.E. Cooper, D.C. Bley, M.T. Barriere,
J. Wreathall, and W.J. Luckas, Jr.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

B.1 INTRODUCTION

Errors of commission (EOCs) were identified as a critical area for development in human reliability analysis (HRA) in our review of operational experience during low power development and shutdown (LP&S) operations.[1] In this task, the following definition for an EOC was developed which is consistent with the refined HRA framework, defined in Appendix A, basic PRA principles, and actual operational experience:

> *An error of commission is an overt, unsafe act that, when taken, leads to a change in a plant's configuration with the consequence of a degraded plant state.*

We recognize that the EOCs of interest do not include all random actions that occur in the plant. Rather, one important goal of this project is to focus more narrowly upon those EOCs that are risk-significant and, therefore, should be included within the scope of a PRA.

The two-fold purpose of this task is: 1) to identify key features of EOCs which can be used to form the basis for quantification methods, and 2) to develop guidance for identifying and modeling EOCs to be included in PRA models. To accomplish these goals, this task was divided into three parts:

- Characterization of potential causes of EOCs and principles for modeling EOCs
- Identification of opportunities for EOCs
- Guidance to HRA and PRA analysts on identifying and representing a focused set of potentially risk-significant EOCs to include in PRA models.

The results of each of these activities, described in detail in the Sections B.2, B.3, and B.4, respectively, will serve as inputs in future efforts to develop methods for quantifying and modeling human errors in HRAs.

The overall results of this task evolved in conjunction with the development of the refined HRA framework (Task 6 - Appendix A) and in parallel with Task 8 (Appendix C) on dependent, unsafe acts. Reviews of operational experience, both LP&S and at-power events, were used to justify recommendations on the basis of data, and to illustrate insights with anecdotal evidence.

B.2 CHARACTERIZATION OF POTENTIAL CAUSES OF EOCS AND PRINCIPLES FOR MODELING EOCS

The following are the specific objectives of this activity:

- Refine guidance on the appropriateness of error types (i.e., slips, mistakes, and circumventions) for EOCs,
- Characterize the causes of EOCs, and
- Identify features required to quantify EOCs.

B.2.1 Analysis Approach

The general approach specified for this task was to use the results of analyses of event data made for this project. The data sources originally specified include analyses of PWR and BWR LP&S events which were reported in earlier draft reports by Brookhaven National Laboratory (BNL)[2] and Sandia National Laboratories (SNL)[3] (e.g., AEOD Human Factors Evaluation reports, Augmented Inspection Team (AIT) reports), and also interviews with subject matter experts. Based upon the analyses performed to date, the most information-rich sources of data are considered to be the PWR LP&S events (both LERs and event reports), and a limited number of at-power events (all event-based reports). The analyses of LERs and event-based reports are discussed separately since the former are more numerous, allowing some statistical investigations to be made, while the reports contain more detailed information but are, in themselves, insufficient for providing statistical insights.

To develop methods for assessing EOCs, the results from data analyses will be compared with the human failure events typically modeled in full-power PRAs; these include pre-accident and post-accident human failure events and are almost exclusively errors of omission (EOC). The pre-accident human failure events, which usually are the result of actions performed outside the control room (i.e., ex-control room) are traditionally modeled using methods considered appropriate for slips (e.g., the Technique for Human Error Rate Prediction (THERP).[4] On the other hand, post-accident HFEs modeled in full-power PRAs are more frequently actions taken inside the control room (i.e., in-control room) and can be both slips and mistakes. Also, human-induced initiators are not modeled explicitly in current PRAs but are captured in initiator-frequency data.

According to the refined HRA framework (see Appendix A) developed in the Improved HRA project, there is a distinction between human failure events and unsafe acts which is relevant when using data on historical events to characterize EOCs. Human failure events are basic events modeled in the PRAs. Their definition depends upon the context of the PRA model (e.g., plant states, type of initiating event), HRA modeling conventions (which may be refined or modified in later Improved HRA project developments), and the preferences of PRA and HRA analysts. Hence, strictly speaking, historical data cannot be used to define EOCs or errors of omission (EOOs) without a specific PRA context. However, such data can be reviewed to identify unsafe acts of commission (UACs) and unsafe acts of omission (UAOs). The relationship between EOCs (or EOOs) and UACs (or UAOs) depends upon the definitions of the EOCs modeled in a PRA and can take several different forms:

- One-to-one (i.e., the definition of the EOC modeled in the PRA is identical to that of an UAC identified in historical data)

- One-to-many (i.e., one EOC modeled in the PRA is defined to represent several UACs identified in historical data)

- Generalization (i.e., the EOC modeled in the PRA is a generalized version of UAC(s) identified in historical data)

Regardless of how EOCs and UACs are related in the context of PRA models, the relationship between them established by the refined HRA framework allows insights on the causes of, influences on, and characteristics of EOCs in general to be gained from investigating UACs in event data. The analysis strategy taken for this task takes advantage this relationship between UACs found in historical event data and EOCs expected to be modeled in PRAs.

Since the available data is relatively sparse, our strategy was to use the database to draw qualitative insights only. In addition, differences in the number of kinds (i.e., initiator, pre-accident, post-accident, recovery) and modes (i.e., commission and omission) of human errors also required that relative comparisons were made, rather than direct ones.

B.2.2 LER-Based Analyses of UACs

The results of LER analyses given in this section on unsafe acts of commission (UACs) are based upon the PWR LP&S full-text LERs coded in the Human Action Classification Scheme (HACS) database.[1] As described above, UACs are identified and investigated in event data in order to infer insights on EOCs.

B.2.2.1 Insights Regarding Error Types

Various "slices" through the HACS database for PWR shutdown events can be used to answer questions such as "what to model?" on EOCs. In particular, differences were investigated between the kinds of errors (e.g., pre-initiator, post-initiator) and error types (e.g., slips, mistakes) for UACs and for unsafe acts of omission (UAOs) which have occurred during LP&S events, as well as differences with the HFEs typically modeled in full-power PRAs. In addition, insights were gained on different events types (e.g., loss of offsite power) with respect to the error kinds, error types, and error modes (e.g., UAC).

Table B.1 shows that UACs are the dominant error mode represented in the PWR LP&S HACS database (i.e., 28 versus 11 UAOs). In addition, UAC initiators are the dominant contributors to the database (18) while UAO initiators are the smallest contributors. Comparisons of the kinds and modes of error for different event types reveal that loss of residual heat removal (RHR) and loss of (offsite) electric power (EP) events during LP&S conditions are more commonly initiated by UACs than by UAOs. For loss of RHR specifically, however, UAC initiators and non-initiators are equally common. In contrast, all UACs associated with loss of EP events are initiators.

Table B.2 examines error types with respect to their kinds and modes. For instance, mistakes and slips are roughly equal in their contribution (10 versus 8) to the eighteen UAC initiators. For UAC non-initiators, mistakes predominate (7 versus 3). In contrast, none of the UAO initiators are mistakes. However, the UAO non-initiators are all mistakes, paralleling the results for UAC non-initiators. Overall, mistakes are more frequent than slips in the PWR shutdown events for both UACs (17 versus 11) and UAOs (7 versus 2).

Tables B.3, B.4, and B.5 give the location of the error along with its kind, mode, and type, and the event type in various permutations.

From Table B.3, UAC initiators outside the control room (i.e., Ex-CR) are the most frequently occurring error mode and kind by location and occur twice as frequently as UAC initiators in the control room (i.e., In-CR). Within the control room, UAC initiators occur twice as frequently as UAC non-initiators. Outside the control room, UAC initiators and non-initiators are closer in number (12 versus 7) but UAO non-initiators out number UAO initiators 3 to 1 (i.e., 6 versus 2). Overall, Ex-CR unsafe acts greatly outnumber in-control room (i.e., In-CR) unsafe acts (27 versus 11) with UAC Ex-CR unsafe acts being the dominant contributors (i.e., 19 of 27 unsafe acts). For UACs, both ex-control initiators and non-initiators occur approximately twice as frequently as the parallel, in-control unsafe acts (i.e., 12 versus 6 for initiators and 7 versus 3 for non-initiators). A similar pattern is seen for UAOs.

Table B.4 examines the location, type and kind of error for UACs only. UAC mistakes occur primarily ex-control (i.e., 13 Ex-CR versus 4 In-CR) while slips occur in roughly equal numbers In-Cr and Ex-CR room (5 versus 6). In the control room, UAC mistakes are more likely to be initiators than non-initiators (3 versus 1), while UAC slips are roughly equal between initiators and non-initiators. The contrary is true for unsafe acts occurring Ex-CR: UAC mistakes are almost equally likely to be initiators or non-initiators while UAC slips are more likely to be initiators than non-initiators.

Table B.5 reports UACs in the PWR shutdown database by event type, and the kind and location of the error. Ex-CR initiators occur predominantly for loss of EP and loss of RHR events. Also, In-CR initiators predominantly result in loss of RHR events. For UACs associated with loss of EP events, there are no non-initiators and Ex-CR initiators comprise the great majority of unsafe acts. In contrast, UACs associated with loss of RHR events occur virtually equally between In-CR initiator or non-initiator and Ex-CR initiator or non-initiator. The only other reasonably strong pattern shown in Table B.5 is that UACs associated with loss of RCS inventory are predominantly Ex-CR non-initiators.

Table B.6 parallels Table B.5 but replaces the location of the error with its type. UAC slips and mistakes occur roughly equally for loss of RHR initiators, while for non-initiators, there is a bias toward UAC mistakes. Similarly, mistakes and slips occur about equally for UAC initiators of loss of EP events. For loss of RCS inventory events, UACs are predominantly mistakes with all UAC initiators being mistakes.

Two significant insights about event types, and error types, mode, kind, and location, are not shown on either Table B.5 or Table B.6. First, UAC Ex-CR initiators for loss of EP and RHR events are evenly split between slips and mistakes. Second, all of the UAC Ex-CR non-initiators for loss of RHR events are mistakes.

B.2.2.2 Insights on Causes of Error

The HACS database for PWR LP&S events can also be used to investigate the error-producing conditions (or performance-shaping factors) important and unique to EOCs. Tables B.7, B.8, and B.9 represent three "slices" through the database investigating the contributions of performance shaping factors (PSFs) to UACs which occurred during LP&S conditions.

Table B.7 examines the contributions of PSFs to error mode (i.e., UACs and UAOs) by location. Paralleling the fact that there are more UACs (28) than UAOs (11) in the PWR LP&S database, this table shows that there are more PSF citings for UACs (52) than UAOs (18). For both there are more PSFs

noted for Ex-CR unsafe acts than for In-CR unsafe acts. Similarly, procedures are cited more frequently for Ex-CR unsafe acts, for both UACs and UAOs, than In-CR unsafe acts. Communications and training are infrequently cited for Ex-CR UACs but infrequently cited for UAOs (both In-CR and Ex-CR). Alternatively, for both UACs and UAOs, human-machine interface (HMI) is cited in roughly equal frequencies for In-CR and Ex-CR unsafe acts. Design citations also are about equivalent for In-CR and Ex-CR UACs, while citations for UAOs are only for Ex-CR unsafe acts. Overall, the order of citation frequencies for PSFs for UACs and UAOs is approximately the same; the two most frequently cited PSFs are procedures and HMI.

Tables B.8 and B.9 examine PSFs for UACs only by location, kind, and type of error. For UAC initiators, Table B.8 shows that procedures are the most frequently cited influence, followed by HMI, then training, communications, supervision, and design. For UAC non-initiators, procedures and HMI are equal in frequency, followed by training and design, then communications. The same general order is observed by location for both initiators and non-initiators. The PSF citings (e.g., initiators versus non-initiators or In-CR versus Ex-CR unsafe acts) cannot be compared directly from Table B.8 because they are expected to be influenced by the different numbers of UACs reported for initiators versus non-initiators and In-CR versus Ex-CR.

Table B.9 shows a similar order of citation frequency for influences. For UAC initiators, procedures is the most frequently cited PSF for both mistakes and slips, followed by HMI and training. For UAC non-initiators, procedures and HMI are cited approximately equally. For initiators induced by mistakes, the top three cited PSFs are procedures, HMI, and communications; the order is similar for initiators induced by slips (i.e., procedures, HMI, training). For non-initiators caused by mistakes, procedures, HMI, design, and training are about equivalent in frequency. For non-initiator slips, procedures and HMI are the only cited influences, and they are roughly equal in importance.

B.2.2.3 Highlights of LER Analyses

As evident in the discussion above, the many "slices" through the PWR LP&S LER HACS database yielded many separate results. Although these results are specific to LP&S conditions, some results may have implications for other conditions and, therefore, represent significant insights which are important to the way in which future PRAs should be performed. The following are examples of such important results:

- UACs occur more frequently than UAOs in LP&S,
- Human-induced initiators, especially UACs, are the most frequent kind of error in LP&S,
- Mistakes are the predominant type of error for UACs,
- Procedures is the most frequently cited negative PSF associated with UACs, followed by HMI, and training, and
- For UAC initiators, procedures is the most frequently cited negative PSF associated with both slips and mistakes.

The implication of these examples is that PRAs, which address all modes of plant operation, should include EOCs, human-induced initiators (explicitly), and mistakes due to their frequent occurrence in

LP&S operational experience. Also, improved HRA quantification methods must continue to address the influence of procedures on human performance. The influences of HMI and training also should be considered. In addition, the implication of the importance of procedures to both slips and mistakes is that improvements in procedures must cover both format and content since slips are commonly associated with formatting, and mistakes with technical deficiencies in procedures.

B.2.2.4 Development of Modeling Principles for EOCs

To develop modeling principles for EOCs, the PWR LP&S data was used to identify factors which are important to representation and quantification.

B.2.2.4.1 Issues Related to Representing EOCs

The solution to the issue of representing human failure events of EOCs within a LP&S PRA must address what kinds of errors are represented (i.e., initiators, pre-accident, post-accident). Ultimately, the representation also must include where the human failure event is placed in the PRA model (e.g., fault trees, event trees). However, we do not discuss placement within the PRA model in this report, but it will be addressed in later tasks for developing quantification methods and HRA guidelines (Tasks 10 and 15, respectively).

Initiators versus Non-Initiators

Previous reports[2] demonstrated that initiators are an important kind of error in LP&S events, which will requiring developing HRA methods. From the discussion above (i.e., Table B.1), UAC initiators were identified as being the dominant mode and kind of error in the PWR shutdown database. UAC non-initiators also were shown to be significant but roughly equal to UAO non-initiators in number.

Overall, there is evidence to support the need to address both initiator and non-initiator UACs for LP&S conditions. In addition, the issue of LP&S human-induced initiators seems almost completely encompassed by the issue of UAC initiators.

Active or Latent Effect

While all of the UAO non-initiators documented in the PWR shutdown database are latent (i.e., pre-accident) errors, UAC non-initiators are equally split between active (i.e., post-accident response) and latent errors. The fact that all UAOs found in the database are latent is consistent with the current modeling practice for full-power PRAs (i.e., pre-accident HFEs that are modeled are typically EOOs). However, the implication for EOCs, is that both pre-accident and post-accident errors must be addressed to accurately represent human performance during LP&S conditions.

B.2.2.4.2 Issues Related to Quantifying EOCs

Historically, the quantification of HFEs can incorporate, either explicitly or implicitly, a variety of factors, such as the kind, type and location of the error, the activity being performed, and the type of personnel. Each of these is discussed briefly below using the information recorded in the PWR LP&S database.

Error Kind (Initiator, Pre-Accident, or Post-Accident)

Usually, for representation, there are different quantification approaches for HFEs of different kinds of error (e.g., THERP for pre-accident HFEs and time-reliability correlations for time-dependent post-accident HFEs). Hence, HRA quantification methods for LP&S PRAs must accommodate each kind of EOC identified as important during LP&S conditions.

Error Type

As shown in Table B.2, mistakes are the predominant type of error for UACs. Consequently, since slips are more commonly modeled in full-power PRAs, new HRA methods which address LP&S must consider EOC mistakes. Preliminary reviews of at-power events suggest that HRA methods for full-power PRAs also should include mistakes.

Action Activity

Tables B.10, B.11, and B.12 investigate the importance of action activity (i.e., operators, maintenance, and testing) for UACs during LP&S conditions.

Table B.10 shows that testing was the commonest activity being performed for UAC initiators, while operations was the second. In addition, UAC initiators caused by testing activities predominantly occurred outside the control room (Ex-CR). Also, mistakes were the predominant error type for both testing and operations-induced initiators.

In contrast, Table B.11 shows that operations were the most frequent activity for non-initiators (both In-CR and Ex-CR), followed by testing. For Ex-CR operations activities, non-initiator unsafe acts were more frequently mistakes than slips; the converse held for In-CR operations activities. All the non-initiators which occurred during testing were mistakes.

Table B.12 shows that both the loss of residual heat removal (RHR) events and the loss of RCS inventory events are most frequently the result of unsafe acts that occurred during operations. Testing also was a significant contributor to loss of RHR events. In comparison, loss of EP events predominantly result from testing activities.

Typically, testing already is reflected in current PRAs as pre-accident errors which leave equipment disabled or misaligned. On the other hand, operations activities typically are only addressed in the post-accident time phase of current PRAs. Our results, given above, indicate that PRAs should consider both EOC initiators and pre-accident errors which result from either testing or plant operation activities.

Personnel Type

Tables B.13, B.14, and B.15 investigate the importance of type of personnel for UACs during LP&S conditions.

As expected, Table B.13 shows that the majority of In-CR UAC initiators can be attributed to licensed operators while the majority of the Ex-CR UAC initiators can be attributed to maintenance/technicians or vendor/contractors. For In-CR initiators, UACs are split evenly between slips and mistakes. For Ex-CR initiators, UACs are more frequently mistakes than slips. Technicians committed the majority of the

Ex-CR mistakes while technicians and contractors made roughly equal numbers of slips. Overall, technicians were responsible for the most UAC initiators and the most mistakes.

Table B.14 has sparse data on UAC non-initiators by type of personnel. However, it shows that the majority of UAC non-initiators were committed by vendor/contractors and that all of these unsafe acts were Ex-CR mistakes.

These results demonstrate that PRAs should consider both CR operators and field personnel in modeling pre-accident, initiator, and post-accident errors.

B.2.3 Report-Based Event Analyses of UACs

Several event-based reports for both at-power and shutdown events have been analyzed in this project and have been coded into HACS (Section B.2.2.2). More recently, these event-based reports were re-visited and analyzed using the data-recording scheme for a specific event, illustrated in Attachment 1. Preliminary results from these more detailed analyses are used in this section to further investigate the causes of EOCs by identifying and analyzing unsafe acts of commission (UACs).

The results from five AEOD reports were judged to be useful in further characterizing the causes of EOCs. The five events addressed are: Braidwood 1 (10/4/90), Loss of RCS Inventory (during LP&S);[5] Prairie Island 2 (2/20/90), Loss of Residual heat removal;[6] Oconee 3 (3/8/91), Loss of RCS Inventory (during LP&S);[7] Crystal River 3 (12/8/91), Loss of RCS Pressure Transient (startup);[8] and Braidwood 1 (12/1/89), Loss of RCS Inventory (transition from cold to hot shutdown).[9] With one exception, all these unsafe acts are UACs. Also, all are mistakes. To utilize all available information on the post-accident response, intermediate recovery actions, which were either sub-optimal or would have been unsafe acts if uncorrected, were included in this analysis. All of the sub-optimal, intermediate recovery actions identified from the above reports of the five events are classified as UAC mistakes.

Our preliminary results suggest that the causes of EOCs differ for unsafe acts which are either pre-accident or initiating events, and those which occur in response to accidents. Consequently, pre-accident and initiating events are discussed separately from post-accident and recovery actions.

B.2.3.1 Insights on Pre-Accident and Initiator Unsafe Acts

Significant pre-accident and/or initiator UACs occurred at Braidwood 1 (10/4/90), Prairie Island 2 (2/20/90), and Oconee 3 (3/8/91) during LP&S operations. The most important influences on the unsafe acts which occurred in these events were performance shaping factors (PSFs) and significant or unusual plant conditions at the time of the event. Table B.16 summarizes the important PSFs (by category only) and significant or unusual conditions for each event and unsafe act. (The number of any multiple effects for the same PSF category identified are shown in parentheses.) The effects of PSFs and conditions on the identified unsafe acts are discussed separately below.

B.2.3.1.1 Performance Shaping Factors

Table B.16 illustrates two important points about to PSFs. First, like the events analyzed from LERs, multiple PSFs were involved in all three events mentioned. All of the PSFs identified were negative influences (i.e., no significant positive aids to task performance were found). Furthermore, several PSFs

are common between the unsafe acts shown in Table B.16.* For example, in the Braidwood 1 (10/4/90) event, the pre-accident and initiating events were coupled temporally (i.e., actions involved were part of same process and occurred close in time), by common personnel, and by common PSFs. Specific negative effects from PSFs which were common to both unsafe acts in the Braidwood 1 event were: 1) Procedures - no procedural guidance for performing two surveillance tests together (the activity in progress), 2) Stress - the two key personnel involved had worked 19 and 17 hours, respectively (i.e., overtime), 3) Communications - in the shift turnover briefing which took place before the unsafe acts it was not stated that two tests were being performed simultaneously, 4) Communications - the engineer in charge of the two tests do not wait for verbal confirmation that the RHR vent valve was closed, and 5) Organizational Factors - normal command, control, and communications were not in force since the control room crew (i.e., shift engineer, shift control room engineer, and board operators) were not aware of the planned changes to the RCS configuration.

In the Prairie Island 2 event, all PSFs which played a role in the pre-accident unsafe acts in assessing the RV level also influenced the initiating event of overdraining the RCS. In addition, the lack of procedural guidance and training on the effects of N_2 pressure impacted both pre-accident unsafe acts and the initiator unsafe act. Common PSFs led to both pre-accident unsafe acts in the Oconee 3 event: 1) HMI - labels on RHR penetration lines (to the sump) were not visible and difficult to access, 2) Procedures - the penetration identification number was not included or required in the procedures for installing the blank flange, 3) Training - the drawings used to identify the penetration lines were not those specified in training, 4) Training - in violation of training guidance, an informal label was used to identify the penetration line, 5) Organizational Factors - lack of control was indicated by the presence of the informal label, and 6) Organizational Factors - the process for procedural writing allowed an incomplete procedure to be used. In addition, the negative influence of organizational factors with respect to complete procedures also applied to the initiator unsafe act in the Oconee 3 event, but applied to the procedure used for surveillance testing of the RHR sump isolation valve rather than for installing the blank flange on the (wrong) isolation line.

The second point illustrated by Table B.16 is that procedures were important to all three events. In all cases, the procedural deficiencies are either lack of completeness (e.g., situation not covered) or no procedure. This type of deficiency underspecifies how tasks are to be performed, representing a gap in guidance which allows undesired variability in carrying out the task. All of the events involved multiple PSFs, so the lack of procedural guidance may also have allowed additional negative PSFs to fill the gap and influence task performance.

B.2.3.1.2 Significant/Unusual Conditions

All three events shown in Table B.16 represent planned activities which did not go as planned and involved some change in the plant's state. Also, all three involved sensitive operations related to changes in the RCS (i.e., breach of RCS pressure boundary or reduction in RV level). For both the Braidwood 1 and Prairie Island 2 events, there were additional unusual circumstances before the initiating event which contributed to the occurrence of both pre-accident and initiator unsafe acts. (Note, the initiating event in both resulted from continuing activities in progress before the initiator.) In the Braidwood 1

* Although all three events also are covered in Table B.10, there are no common PSFs between the pre-accident and initiator unsafe acts shown in Table B.9 and the post-accident and recovery actions shown in Table B.10.

event, two surveillance test procedures were being performed simultaneously for the first time. Lack of procedural (and administrative) guidance and prior experience in performing the tests together were significant contributors to the occurrence of this event. The Prairie Island 2 event also involves previously unencountered conditions. The N_2 pressure was higher than normal, requiring calculations of RV level to involve extrapolations from lower N_2 pressures. In addition, on previous occasions, experienced draindown crews performed RCS draindowns (assisted by an experienced systems engineer). In the Prairie Island 2 event, both the draindown operators and the assisting systems engineer were inexperienced. In contrast, the Oconee 3 event was set up by the pre-accident unsafe acts (i.e., a cascading-type dependency) and the actions involved with the initiator merely triggered the eventual discovery of the pre-accident unsafe acts.

B.2.3.2 Insights on Recovery Actions

All five event-based reports were useful in characterizing causes of post-accident EOCs through the identification and analysis of unsafe acts of commission (UACs). Both recovery actions and intermediate, sub-optimal actions are discussed in this section.

Reviews of the five events suggest that PSFs and cues for diagnosis are the important influences on the opportunities for post-accident and recovery UACs. Although Table B.9 shows that both the Braidwood 1 (10/4/90) and Prairie Island 2 events involved significant and unusual conditions, these conditions no longer existed at the time of recovery. Consequently, plant conditions do not seem to be as directly critical to recovery actions as they do to pre-accident and initiator unsafe acts. In addition, examination of the diagnosis involved for recovery in the five events indicated that cues for diagnosis should be separated into three categories: misleading, discounted, and used and useful. Table B.10 summarizes preliminary results, which are discussed in more detail below.

B.2.3.2.1 Performance Shaping Factors

Table B.17 illustrates three points about the influence of PSFs on the responses to accidents. First, like pre-accident and initiating unsafe acts, multiple PSFs are active for many of the actions shown in Table B.17. However, it also shows that most of the PSFs which play a role in recovery actions are positive factors in task performance. In fact, only positive PSFs were identified for the successful recovery actions while the intermediate, sub-optimal actions had only one or two negative PSFs in addition to positive PSFs. Comparing Tables B.16 and B.17 reveals that instrumentation plays a more important role in recovery actions than in pre-accident and initiator unsafe acts. Its importance is consistent with the importance of diagnosis and cues for diagnosis for recovery actions.

B.2.3.2.2 Diagnosis Cues

Diagnosis cues primarily consist of control room instrumentation and reports from the plant (e.g., local indications reported by phone). Both the availability and the interpretation of these cues influence the ability to correctly diagnose accident conditions (and confirm successful recovery actions). Consequently, the three categories of diagnosis cues were developed to account for: 1) misleading cues (e.g., failed or flawed instrumentation) or misinterpreted information, 2) accurate information that is rejected, and 3) helpful information that leads to successful recovery.

Table B.17 illustrates diagnosis for two different kinds of events: 1) for two events, only successful recoveries were identified and 2) for the other three events, sub-optimal actions were identified, as well as successful recovery actions.

Immediate, successful recoveries were achieved in both the Braidwood 1 (10/4/90) and Prairie Island 2 events. No intermediate, sub-optimal actions were identified. Also, all of the PSFs were positive for these events and all of the accident cues were unambiguous and were acted upon (i.e., only "used & useful" cues).

Sub-optimal actions, negative PSFs, and misleading cues were identified in the Oconee 3, Crystal River 3, and Braidwood 1 (12/1/89) events. In addition, useful information was rejected or discounted in the initial response to the Oconee 3 and Crystal River 3 events. Reviews of the event timelines and operator interviews given in the reports for all three events revealed that an initial, erroneous mindset had to be overcome before successful recovery was achieved. Furthermore, misleading cues were used to support the initial erroneous mindset in all three events while useful information which was inconsistent with the mindset was initially discounted in the Oconee 3 and Crystal River 3 events. Successful recovery in all three events appears to have resulted from an "initial mindset breaker" - either a single, unrefutable cue or the accumulation of information.

In the Oconee 3 event, both the high level alarm on the reactor building's emergency sump and the decreasing RV-level indication were discounted. According to the Oconee 3 event timeline, operators conjectured that the RV level transmitter was malfunctioning. In addition, the high level alarm was attributed to washdown operations which occurred earlier in the outage. Based upon these interpretations of information, it is surmised that operators did not initially recognize the existence of an RCS drainpath. Reports from the reactor building on the decreasing RV level and increasing radiation appeared to be the factors convincing them that there was an RCS drainpath. Awareness of the tests on the RHR sump isolation valve and the indication that the RCS level was not increasing, even with injection from the Borated Storage Water Tank (BWST), eventually lead operators to close both RHR sump isolation valves, terminating the draining of the RCS. Indication of increasing RV levels after isolation of the sump valves confirmed the success of the final recovery actions.

In the Crystal River 3 event, the initial mindset attributed the decrease in RCS pressure to cooling (i.e., shrinkage of the coolant and a lower pressurizer level and pressure). This mindset was erroneously supported by the report of steam flow to the deaerating feed tank and indication that the pressurizer spray valve was closed (although it was open, in fact). Because the misleading cues confirmed the initial mindset, trends in pressurizer level and RCS temperature were discounted. Instead, reactor power was increased several times (in attempt to compensate for the perceived RCS cooling condition) and automatic ESFAS actuation was bypassed for 6 minutes. The "mindset breaker" consisted of the combination of (1) continued observation of trends in RCS pressure and pressurizer vapor space temperature, with variations in high pressure injection flow, and (2) a remembered rule that closing the pressurizer spray block valve was one response to decreasing RCS pressure.

As shown in Table B.17, a substantial amount of "used & useful" information was available in the Braidwood 1 (12/1/89) event. However, a report of a leak in the vicinity of the RHR A train relief valve supported the initial mindset of assuming that the operating RHR A train was responsible for the RCS leak. Training and engineering practice was the reported origin of this mindset. The ultimate mindset breaker was a field report of flow through the RHR B train relief valve in combination with continued increases in the holdup tank level and decreases in RCS pressure until the RHR B train was isolated.

2.3.3 Implications

Several important implications can be drawn from the results of these report analyses. Some implications are specific to the time-phase division (i.e., pre-accident and initiator versus post-accident) established at the beginning of this section. Others establish a common connection between unsafe acts committed in all time phases. If such common factors can be identified, an important step forward can be claimed in the effort to improve HRA and PRA methods.

Two important insights can be drawn from the analyses of pre-accident and initiator unsafe acts. First, the consistency of results on PSFs between all five events (as well as the LER results) implies that, under current plant practices and the present regulatory environment, it is reasonable to expect that multiple, negative PSFs are likely to influence most activities performed during LP&S. Consequently, the stage already is set and, given the opportunity, an EOC is likely to be committed. Second, the opportunities for EOCs, which are addressed further below, are defined by the activities which involve plant interventions and the conditions under which they are performed. Examples given above of significant or unusual conditions associated with pre-accident and initiator unsafe acts correspond with both activities and plant conditions.

From our discussion above on post-accident unsafe acts, the role of diagnosis cues in confirming an initial, erroneous mindset and in breaking that initial mindset can be compared to the concepts of similarity-matching and frequency-gambling in memory retrieval (see, for example, Reason[10]). All three cases in which sub-optimal recoveries occurred, a mindset prevailed as the initial diagnosis to the event, which seemed to be derived from past experience or training. In some cases, initial indications matched this initial mindset, confirming this erroneous diagnosis. The break from the initial mindset was achieved only after completely unambiguous and/or cumulative evidence to the contrary was provided.

Bley[11] noted that there appear to have been common factors in the most notable events which have occurred in nuclear power history (e.g., Chernobyl, TMI-2) which are also common to the events (particularly LP&S) analyzed for this project:

- The plant is operated outside the designer's intentions;
- The plant then enters a regime where its behavior is not understood; and
- Operators refuse to believe accumulating evidence.

These elements are particularly noticeable in the events shown in Tables B.16 and B.17. For example, insufficient guidance in procedures for many of these events led to unproceduralized actions which deviated from good operating practices (especially Braidwood 1 in which two procedures were performed simultaneously). Also, insufficient understanding of plant's behavior is evident in the Prairie Island 2 event (e.g., misunderstanding about high N_2 pressure) and in the Crystal River 3 event (e.g., lack of understanding as to the cause of the RCS pressure transient). In other events, there seemed to be a lack of sensitivity to the importance of changes in RCS configuration (e.g., planned breaches in RCS pressure boundaries in Braidwood 1 and Oconee 3 events). The two of the three events which involved sub-optimal recoveries shown in Table B.17 illustrate situations in which operators refused to believe instrumentation which was, in fact, providing reliable information.

B.3 IDENTIFYING POTENTIAL OPPORTUNITIES FOR EOCS

The work described in this section further supports the development of guidance for treatment of errors of commission (EOCs) to be modeled in PRAs. Specifically, the stated purpose of this activity is "...to select or develop a process for systematically identifying the opportunities for EOC for both full-power and LP&S operations." As in other project tasks, developing the EOC identification scheme described in this section is based upon concepts established in Task 6, Refine [HRA] Framework (see Appendix A).

B.3.1 Approach

The approach to identifying EOC opportunities is an extension of the insights derived from reviewing operational experience, described in the previous section. In particular, two different approaches are recommended for different time phases, based on our discussion in Section B.2.3.

We described previously that, for pre-accident and initiator unsafe acts (especially during LP&S), the "stage is already set" for EOCs to be committed, and that the only additional factor needed was the opportunity. In other words, in the present industry and regulatory environment, it is probably not necessary to investigate features of PSFs which would be in effect when an EOC is committed; it is reasonable to infer from operating experience that current plant conditions will include multiple, negative influences on human performance. However, the opportunities for EOCs are a function of the plant's design, conditions, and activities.

On the other hand, the previous section described both cues for diagnosis and the existence of an initial mindset as the important factors in EOC occurrences in the post-accident phase. Control room instrumentation is the most frequently used source of information to prompt operators to perform appropriate accident responses, although not the only source. Recollections of training and procedures comprise the likely sources of initial mindsets. In addition, procedures usually refer to instrumentation to be used in responding to accidents. Based upon this discussion, two approaches to searching for EOC opportunities are recommended:

1) **Mechanism Search**. For pre-accident or initiator unsafe acts, a defense-oriented approach is suggested based upon a plant's design and configuration, coupled with an investigation of controls (or limits) on plant conditions, especially unusual or previously unencountered conditions, and activities, and

2) **Procedure Search**. For post-accident unsafe acts and some initiators, an approach to searching procedures is recommended that includes considering uncertainty at decision points due to instrumentation that may be both helpful and applicable in diagnosing an accident and its time sequence. The focus of the search would be on emergency procedures for post-accident unsafe acts and on outage procedures for LP&S initiators.

Both the mechanism and the procedure search approaches are discussed further in Sections B.3.2 and B.3.3.

The controls on plant conditions and activities can be investigated either directly through the quantification process (addressed in future work) or by searching administrative procedures governing the performance of activities for both at-power and outage operations. Treatment of instrumentation in

both identifying and quantifying EOCs was recognized as an important issue which will require further assessment in future work. At present, failures of instrumentation due to pre-accident or initiator unsafe acts can be treated identically to failures of equipment. However, the possibility must be recognized of human-induced failures of instrumentation due to, for instance, organizational factors that lead both to their disabling and to their demand before return to service. In addition, procedural references and control room walkdowns can be used to identify the instrumentation important to diagnosing specific events.

An exception to the scheme for identifying EOC opportunities is for loss of RHR events initiated by overdraining the RCS when going to mid-loop. These particular initiators share many similar features with typical post-accident unsafe acts: good instrumentation, procedural guidance, and training are critical. Consequently, it is recommended that these unsafe acts be investigated by both approaches.

B.3.2 Mechanism Search: A Defense-Oriented Approach for Assessing the Impact of Plant Conditions

Plant conditions (e.g., RCS parameters, system configurations, plant operating mode, activities in progress) constrain or define the opportunities for EOCs. A strategy for characterizing the potential for unsafe acts at some level between top-level failure definitions (e.g., loss of RCS inventory) and anecdotal data (e.g., the Oconee event) is useful to identifying opportunities for EOCs (Task 7 - this Appendix) and the potential for dependencies between unsafe actions (Task 8 - see Appendix C). This strategy is described as a defense-oriented approach in which system or plant functional failures are decomposed (for example, using fault trees) to search for accident sequences (probably plant-specific). Such accident sequences represent the ways in which failures in plant functions can occur (e.g., RCS boundary integrity).

For example, a search for ways to reduce reactor vessel (RV) level during LP&S operations should include both the potential for drainpaths and the potential for over-draining. Based upon system configuration and hardware under the range of plant conditions during LP&S operations (e.g., typical activities, system operating configurations), the search process should identify potential drainpaths which involve both single and multiple failures. Three separate searches for drainpaths are recommended to examine separately the potential of single and multiple failures (including dependencies), and In-CR and Ex-CR unsafe acts. Drainpaths which are initiated Ex-CR are likely to be single failures for which the recovery is finding and isolating the leak. Drainpaths created as the result of both In-CR and Ex-CR involve will consist of multiple, probably dependent unsafe acts. In addition, while their recovery will be similar to that for a single unsafe act, it also may be complicated by a requirement in overcoming a mindset that "two defenses cannot be defeated" and by the fact that the same personnel who initiated the event must now respond to it. Draindowns initiated from the control room (such as the Prairie Island event) are similarly complicated because they involve the same personnel both in the initiator and in the required response. Operating experience shows that in all three cases, two kinds of errors cause difficulties for operators. Ex-CR operators sometimes open the wrong valve (a slip); sometimes, when opening the right valve, a draindown path is created because other valves had been mispositioned previously (a latent failure, and probably a slip). The CR operator's "knowledge" that the right valve was operated and that it could not cause draining creates a mindset that refuses to accept the possibility of a link between current operations and the loss of coolant.

Part of the search process is to generalize the information from tokens (specific events) into classes of human errors that must be modeled in PRA. Developing event sequence models for the process that lead to the token appears to be a viable approach to understand and generalize these events.

B.3.3 Procedure Search: An Approach for Assessing the Impact of PSFs, Plant Conditions, Instrumentation, and Sequence Timing

Following the assessment using the above defense-oriented approach, plant conditions, PSFs, and instrumentation should be examined for how these factors can be "triggers" of EOCs. Event data can be used to develop the general characteristics of potential deficiencies in these factors which can lead to an EOC. However, as stated above, we anticipate that the major part of the process for identifying EOC opportunities will consist of plant-specific examinations. For example, the procedures used for testing valves that serve as RCS boundaries can be reviewed to identify which drainpaths are more likely and to identify potential dependencies between actions involving valves on the RCS boundaries (e.g., same procedure, same location).

No specific tools have been developed for identifying triggers associated with plant conditions, PSFs, and instrumentation. However, a search method is under development that is intended to find error-prone conditions in procedures. For example, this method is expected to be able to assess how well procedures cover specific transients (e.g., small LOCAs, loss of service water), conditions, or situations (e.g., transitions to full-power) out of the larger class for which the procedure serves. Preliminary work has indicated that the following conditions can create the potential for EOCs:

- Emergency procedures are developed for nominal accidents that have been analyzed in great detail
- Emergency procedures have been extensively tested against the nominal accidents
- Specific differences in plant parameter response and timing due to plant-specific differences in design and accident-specific details of the initiating event and initial conditions can lead to improper or vague sequencing of decision information vis-a-vis the procedure's decision points; in turn, this requires circumvention, or paralysis ensues

In the procedure search there will be times, especially for LP&S, when they will be found to be deficient, i.e., they contain gaps and incomplete cautions or guidance. In such cases, the search amounts to little more than a review of the procedure against accident requirements. However, when the procedures are good (i.e., are complete and executable) the most likely problem is one in which, arriving at a decision point in an emergency procedure, the plant conditions anticipated by the procedure have not yet been met or are difficult for the operators to identify because of timing, instrumentation, or situational pressures. Typically, the procedures do not return to such decision points for continued verification. To identify such conditions, it is necessary to include realistic consideration of possible plant accident trajectories and actual criteria for emergency procedure decisions.

Two search venues would appear to be warranted. First is an examination of plant emergency procedures to identify decision points, including searching them for cases in which uncertainties in timing, parameter values, and instrumentation, allow opportunities for committing to improper or less desirable actions. Presently, estimates of the effects of timing, etc. are based on judgement by those with operating experience and knowledge of physics calculations for accidents. The project is looking for classes of events and definition of search strategies, not perfection in searching a particular plant. During later

tasks, plant specific-searches will be performed, and refinement with plant-specific thermal-hydraulic analysis will be justified in some cases.

Second, if records (such as crew debriefings and EPRI data) of simulator exercises are available, a search for EOCs and explanations of why they occurred could provide additional information.

To clarify the current status of the process of procedure search, we consider the following outline of the strategy. The search must be done on a test case by searching procedures for one specific plant.

- List the PRA initiating events to be considered. Select a subset of those in the full power and LP&S PRAs, choosing those where timing could strongly affect decisions and the likelihood of success. For each specific initiator, develop a thermal-hydraulic/plant response time-line to document the expected progression of plant parameters for the accident.

- Define the plant conditions that should cause operators to begin each procedure. Identify any possible decision-confusion points; e.g., are there multiple procedures with nearly identical entry indications?

- Construct a flowchart defining the expected order of procedure usage for each initiating event or each initiating event/event sequence pair.

- Define the expected plant response to each initiating event or each initiating event/event sequence pair in a flowchart of procedure decision points.

- Cull the list of decision points according to coarse screening criteria; i.e., likelihood and consequences.

  - Are there significant consequences of a possible wrong decision? If not drop that decision point from further consideration. Consider consequences of the decision itself and those evolving from a strong influence on ensuing decisions and actions.

  - Is the decision clear, or are there factors such as uncertainties in indications or the point in time when this decision point is reached that strongly affect selection of the expected option. That is, considering the range of possible detailed sequences arriving at this point, how likely is a wrong decision? If plant conditions and uncertainty in the decision criteria are unlikely to be important, then drop that decision point from further consideration.

- For the surviving decision points, develop a table listing the decision criteria, their expected values when the decision point is reached, and the uncertainties associated with the indications and the timing. Consider what aspects of the accident sequence dynamics could lead to improper sequences of action (i.e., EOCs).

B.4 GUIDANCE TO HRA AND PRA ANALYSTS FOR MODELING EOCS

Using the results discussed above, the development of preliminary guidance for HRA and systems analysts is described in this section. Specifically, this guidance discusses how to identify which EOCs should be included in PRA models and how to represent them in the model.

B.4.1 Approach

The goal of this activity is to support the expansion of the unsafe acts beyond those currently modeled in PRAs to include explicitly EOCS that were previously unmodeled. The systematic process developed will be bounded in include those EOCs expected to be important, as described in previous sections. It is envisioned to involve "rules" for identifying and modeling EOCs. Development of these rules will to be an evolving process. The initial guidance for EOC identification and representation tasks will be based on the rationale for current modeling of human failure events (HFEs), the experience from operational events, and concepts underlying the revised framework. The guidance on identifying EOCs given in this section should be used in conjunction with the search methods for identifying opportunities for EOCs, discussed in the previous section.

This section uses the information that was summarized in Attachment 1 on the loss of RCS inventory event at Oconee, Unit 3 (3/8/91),[7] to illustrate points made in the discussions.

B.4.2 HRA/PRA Modeling Rules

Rules for modeling human failure events in PRAs should ensure that risk-significant ones are included in PRA models. Their risk significance should govern both how these human failure events are represented in PRAs and how they are quantified. Current rules for modeling human failure events in PRAs are examined to discuss the underlying rationale for assessing their risk significance. These rules are re-examined in the context of the operational experience which was analyzed and discussed in earlier sections of this report. Finally, the concepts developed in the refined HRA framework (Task 6 - Appendix A) are used to extend the application of the rationale used in current PRAs to that for future PRAs addressing all plant operating modes.

B.4.2.1 Current Rules for Modeling Human Failure Events in PRAs

The guidance for modeling human failure events in current full-power PRAs recognizes two different effects of error: pre-accident and post-accident. Pre-accident human failure events that are modeled typically represent the disabling of safety equipment (i.e., inadequate restoration of components after required proceduralized testing or maintenance). Post-accident human failure events which are modeled are those actions which, if not performed, lead to core damage in the absence of successful, alternate hardware operation or independent actions. Human-induced initiators are not explicitly modeled. Rather, they have been subsumed in the initiator-frequency data (i.e., implicitly modeled) because such human failure events are claimed to be infrequent and captured adequately by such data.

In current PRA models, pre-accident human failure events often are implicitly modeled as slips, and may be either EOOs or EOCs. The current guidance for modeling them usually implies that these events are defined as independent, both from other pre-accident events and from post-accident events.[12] Furthermore, pre-accident events infrequently require refining beyond screening values, i.e., no detailed analysis is required.

On the other hand, post-accident human failure events modeled in current PRAs are typically omissions of actions. Current modeling practices can imply that they are either slips or mistakes. However, the time available for response is frequently the more dominant factor influencing human reliability results. Cutsets generated from full-power PRAs frequently contain only one post-accident human failure event (i.e., a human was the final defense for preserving and maintaining some plant function). Multiple human-failure events (including non-recovery events) which occur in cutsets can be either dependent or independent. Justification for modeling them as independent events typically is based upon time separation, different personnel, or a different plant function and location (e.g., restoration of offsite power and residual heat removal (RHR) switchover to recirculation). Treating dependencies between post-accident human failure events in current PRAs often is limited to factors such as common cues for diagnosis and common available time limitations.

B.4.2.2 Connection With Event Data for EOC Unsafe Acts

Using the analyses of operational experience discussed in Section 2, human performance in actual events can be compared with that reflected in current PRA models. Some of this discussion will be given in the context of the refined HRA framework (See Section B.4.2.3 below). In this section, the rationale underlying current HFE modeling in PRAs will be generalized and applied to LP&S operations and to the specific features of these full-power events that have been analyzed.

Whether it be current, full-power PRA models or improved PRA models for various modes of operation, risk significance is the key to bounding the set of unsafe acts to be modeled, including EOCs. Detailed HRA modeling in current PRAs focuses upon errors of omission, post-accident events, and dependent events. The focus upon errors of omission can be explained by the plant state or operating mode. During normal conditions in full-power, there are relatively few human interactions with the plant i.e., opportunities for initiator or pre-accident unsafe acts.

However, after an accident sequence has been initiated, certain actions are usually required by the operators (i.e., they must act). If these actions are omitted, core damage is expected to occur. The correct actions to be performed are prescribed by emergency operating procedures (EOPs). In contrast, errors of commission can be described as inappropriate, rather than the lack of, interactions with the plant. The key question, then, is "why act?" Two reasons suggested by the reviews of LP&S and full-power events are 1) personnel are already interacting with the plant, or 2) the interpretation of plant's symptoms by personnel leads them to believe that interaction is required. Reviews of the operational experience show that procedures are the dominant influence on LP&S unsafe acts in general, including UACs, and, therefore, on EOCs by virtue of their relationship to UACs established in the refined HRA framework. However, the procedures are frequently either incomplete or nonexistent. Other performance shaping factors (PSFs) found to be important to UACs in LP&S events are human-machine interface (HMI) and training. In addition, instrumentation is an important contributing factor to UACs both during LP&S operations (e.g., reactor vessel level indication during mid-loop operations) and during response to full-power accidents (e.g., reactor coolant temperature and pressure, sump-level indications).

Reviews of LP&S and full-power events for UACs also identified important dependent relationships between unsafe acts. However, the relationships found in these events include dependencies across time phases, e.g., pre-accident/initiator, pre-accident/post-accident dependencies. For example, as previously shown in Attachment 1, pre-accident UACs set up the initiating event in the 1991 Oconee Unit 3 loss of residual heat removal (RHR) event. Also, common organizational processes may have caused a suboptimal response to the loss of RHR experienced in at Oconee.

Errors of omission (EOOs) are defined as not performing an action as specifically described in Emergency Operating Procedures (EOPs). Thus, there usually is only one way to correctly perform the action prescribed by the EOP and, therefore, there is a fairly specific definition of the EOO. In contrast, historical data (LP&S and full-power events) suggests that errors of commission (EOCs) frequently occur as the result of lack of specification in procedures, e.g., incomplete procedures or no procedure. Without the procedural specification of the unsafe act, EOCs must be defined by the plant and system functions which it defeats. Consequently, since there can be a variety of ways to defeat plant or system functions, the definition of EOC events will be more general than that for EOOs.

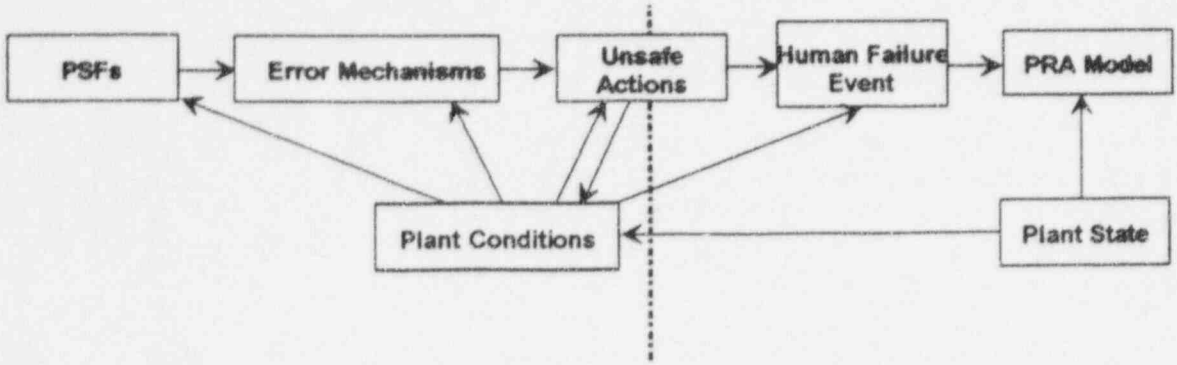
B.4.2.3 Connection With the Refined HRA Framework

To develop rules for identifying and modeling risk-significant EOCs, it is important to understand the factors influencing their occurrence. The rules of identifying and modeling EOCs will vary with the influence of these factors; the principal ones are illustrated in the refined HRA framework developed in Task 6 (see Appendix A) and shown in Figure B.1. These factors include plant conditions, plant state, error types, and PSFs. The following are examples of differences in rules for these factors:

- Rules for EOCs during LP&S operations may differ from those for full-power operations,
- Rules for losses of electric power may be different than those for loss of RHR,
- Rules for initiators may differ from those for post-accident unsafe acts,
- Rules for mistakes may be different than those for slips, and
- Rules about the impact of PSFs may be different for full-power in which available time and procedures are dominant contributors, than for LP&S in which multiple influences are common.

Plant conditions can constrain or create the opportunities for EOCs both at a top level and more specifically. At a general level, plant conditions, recognized as "plant states" by the PRA, can define the general potential for EOCs based upon the characteristics of plant operations in different modes. For example, in cold shutdown, there are many more interventions with the plant which represent opportunities for EOCs. On the other hand, Figure B.1 shows that plant conditions can represent a more specific set of circumstances which constrains or creates the options or opportunities which, in turn, are modeled as specific unsafe acts in a PRA. Section B.2 shows some results from the HACS database which indicate the different characteristics of UACs committed during different types of events. For example, Tables B.1 and B.5 show that UACs associated with loss of electric power events are predominantly ex-control room initiators while those associated with loss of RHR are fairly equally split between initiators and non-initiators and In-CR and Ex-CR room actions. In addition, some plant conditions, e.g., high decay heat, may define the risk significance of the consequences of opportunities for EOCs.

Figure B.1 also shows that there is a relationship between plant conditions and error types. For this portion of the refined framework, plant conditions serve as the stimulus for plant interventions which can result in different types of errors. The loss of RHR events at Oconee 3[7] and Prairie Island 2[6] illustrate different conditions which lead to mistakes. In both cases, the UAC initiator was the result of a mismatch



HRA, Human Factors, Behaviorial Science, & Plant Engineering

PRA

Figure B.1 Multidisciplinary HRA framework

between the actual and perceived plant conditions. In the Oconee draindown event, the initiating event, as well as the two pre-accident unsafe acts which set up the initiator, were mistakes (see Attachment 1). The pertinent initial plant conditions for the Oconee event were: refueling complete, RHR maintained by one RHR pump, reactor vessel level 12 feet above core, and maintenance and surveillance testing planned for one of the two RHR sump isolation valves. In particular, the Oconee event was initiated due to the combination of the planned testing of the sump isolation valve and of the mismatch between the actual and the perceived plant condition about which sump isolation line was blocked. In the Prairie Island over-draining event, the initiator, again set up by pre-accident mistakes, also was a mistake. In contrast, the initial plant conditions for Prairie Island were high decay heat, RCS draindown to mid-loop in progress, the unavailability of a newly installed level indication system on the reactor vessel that was unknown by operators responsible for draindown, and one poorly human-factored source of vessel level indication. The simple fact that draindown to mid-loop was in progress (i.e., planned intervention) provided the opportunity for unintentionally overdraining, thereby leading to loss of RHR.

As illustrated in Figure B.1, performance shaping factors (PSFs) impact error mechanisms in a fashion similar to plant conditions. According to LP&S event data, incomplete, inaccurate, or non-existent procedures, are the most frequently cited contributors to UACs, including those in the Oconee 3 and Prairie Island 2 events. Human-machine interface deficiencies, such as the poor visibility of the reactor vessel's level indication used in the Prairie Island event, is the second most frequently cited negative influence on human performance. Table B.9 shows that both procedures and HMI are equal contributors to initiator slips and mistakes and non-initiator slips and mistakes. Since the procedures used in the Oconee event did not provide instructions on identifying the correct penetration line, the contribution from procedures in installing the blind flange and making two independent checks on the installation was only to verify the originally selected (and erroneous) intention of installing the flange on the wrong suction line. The negative impact of HMI in the Oconee 3 event (i.e., labelling of penetration line) also was related to mistaken intentions, rather than slips in implementation, since the wrong information (i.e., informal label, flow diagrams) was used to identify the original penetration line. On the other hand, in the Prairie Island 2 event, procedures led both to the pre-accident mistake in calculating and interpreting the level in the reactor vessel and to the initiator of overdraining (i.e., unintended overdraining).

B.4.3 General Guidance for EOC Modeling

Using the discussions concerning the refined HRA framework and preliminary insights from data analyses, a candidate set of rules was devised for identifying a limited scope of risk-significant EOCs to be included in PRA models that is compatible with, and builds upon current HRA modeling practices. As noted above, EOCs are such that some generalization in their modeling is expected. Consequently, the following general guidelines are suggested for modeling EOCs:

- Consider EOCs separately for different plant operating modes (e.g., full-power, startup, shutdown) and different event types (e.g., loss of electric power, loss of RHR),
- Examine plant conditions which are characteristic of each plant mode to identify the reasons or opportunities for plant intervention,
- Investigate task- or intervention- specific PSFs, plant conditions, and instrumentation issues as possible triggers for inappropriate plant interventions, and
- Give special attention to dependent unsafe acts; in particular, all typically modeled classes of unsafe acts (i.e., pre-accident, post-accident) should be modeled as usual, supplemented by those initiating and pre-accident events which have dependencies with other events.

This general guidance for limiting the scope of EOCs to be modeled should be considered in conjunction with methods for identifying EOC opportunities, described in the previous section. Further guidance specific to different plant operating modes and event types is given next.

B.4.4 Rules for Specific Plant Operating Modes

This section summarizes preliminary insights from data analyses which are pertinent to identifying risk-significant EOCs to be included in PRA models. Full-power and shutdown operating modes are considered separately. Also, when data analyses can support them, distinctions are made between different definitions of accident sequences (i.e., event types).

B.4.4.1 Shutdown

Five major event types were represented in the LP&S events analyzed: loss of electric power (EP), inadvertent ESFAS actuations, loss of RHR, loss of reactor coolant system (RCS) inventory, and inadvertent additions to reactivity. Features pertinent to opportunities for EOCs are briefly described below.

As shown in Table B.1, all of the UACs involved in loss of EP and inadvertent ESFAS actuations are initiators. Tables B.5 and B.15 also show that the UAC initiators in loss of EP events are pre-dominantly ex-control room actions performed by maintenance, technician, or vendor/contractor personnel. In addition, of all the LP&S events, loss of EP is the only type for which there is an automatic safety equipment response, i.e., the emergency diesel generators start. Furthermore, recovery from these events generally appeared to be straightforward and no dependencies with other unsafe acts were apparent. Consequently, since human-caused loss of EP events are indistinguishable from hardware-caused loss of EP events, we recommended including the EOCs for these event types in initiating-event frequency data, rather than explicitly modeling them. Based upon the limited data on inadvertent actuation of Engineered

Safety Features Actuation Signal (ESFAS) events, it is recommended that EOCs for this event type get treated similarly. However, explicit PRA modeling of EOCs for both of these types should be considered in cases for which dependencies could exist with other human actions, such as under abnormal conditions in which the control room's instrumentation or indication is unavailable.

According to preliminary analyses of BWR LP&S event data, inadvertent reactivity addition events are predominantly In-CR unsafe acts performed by licensed operators. Although there are relatively few, EOCs (predominantly initiators) associated with these events should not be ignored. Specific guidance will be developed in later tasks.

Losses of RHR and RCS inventory events are discussed together since that latter can lead to losses of RHR. Other similarities between these events are illustrated in various tables discussed in Section B.2. For instance, as shown in Table B.1, the majority of all UACs identified in LP&S events are associated with loss of RHR or loss of RCS inventory events. In both cases, the numbers of UAC initiators and non-initiators are about equal. According to Table B.5, UAC initiators of RHR or RCS inventory losses can be In-CR or Ex-CR. Consequently, top-level guidance to identify EOC opportunities for these two event types is to consider all error effects, i.e., pre-accident, initiator, and post-accident, all personnel types, all locations, and all types of error.

B.4.4.2 Full Power

Based upon preliminary analyses of full-power events, the top-level guidance is to focus on transients or other event types for which interpretation of CR indicators can be ambiguous. Such ambiguous indication can lead to either erroneous or delayed diagnosis. In general, human-induced initiators, EOC or otherwise, have not appeared to be important during full power events.

B.4.4.3 Startup/Less-Than Full Power

Preliminary analyses of event data for startup or less-than full power events suggest the same treatment as for full-power events. In addition, during these conditions, there is the potential for (1) RCS drainpaths (the result of Ex-CR actions, primarily) and (2) the discovery of pre-accident unsafe acts disabling equipment or instrumentation.

B.5 CONCLUSIONS

The work described in this report provides valuable insights about EOCs which both furthers our understanding of human performance in general, and paves the way for developing HRA quantification methods and guidance in future project tasks.

From our data analyses performed, it was demonstrated that UACs and, by inference, EOCs occur in both LP&S and at-power events. These UACs are not act of sabotage. Rather, they are unsafe acts which are consistent with the traditional HRA definitions of events which should be modeled in PRAs. These UACs are risk-significant actions which are involved in the response to accidents either directly or indirectly, through dependencies between unsafe acts. Consequently, such UACs deserve explicit modeling in PRAs as EOCs.

This work demonstrated that the previously perceived infinite sink of EOCs, can be bounded. Certain EOCs can continue to be modeled implicitly in PRAs through initiating event frequencies and hardware unavailabilities. The EOCs which should be explicitly modeled in PRAs can be found through the approaches for identifying opportunities for them. The continuation of this project will refine guidance on which EOCs to explicitly or implicitly model, and appropriate (e.g., EOP) search techniques.

The causes of EOCs can be characterized using the refined HRA framework developed in Task 6 (see Appendix A). This work included an investigation of a familiar set of influences on the UACs identified in PWR LP&S LERs and event based reports. However, identifying important EOC characteristics required a break from the familiar perspective on human reliability influences and the underlying assumptions of PRA models. For instance, plant conditions, defined at a more detailed level than currently used in PRA models, were shown to be important influences on both human performance and accident consequences in LP&S events. For at-power events, the specific physical conditions in the plant for actual events of certain classes which involve EOCs (e.g., transient, small break LOCAs) may not be recognized or well understood. Consequently, these plant conditions may not be explicitly considered by either plant procedures and training or by the PRA model.

This work also showed that instrumentation cannot always be assumed to be available and reliable (especially during LP&S conditions and during changes in plant state). Furthermore, interpreting instrument indications and implementing procedures cannot be assumed to be correct or uniform under the variety of possible plant conditions. Based upon the results of this project thus far, plant conditions, PSFs, and instrumentation are important factors in the identifying, representing, and quantifying EOCs.

In summary, rationality and order can be brought to the modeling of EOCs. The work completed thus far, and that planned for the future will be a stepwise improvement in current PRA modeling practices, rather than a complete departure from them.

Table B.1 Number of Initiator & Non-Initiator UACs* & UAOs by Event Type**

Error Mode→	UAC			UAO			Total
Error Kind→	Initiator	Non-Init	Total	Initiator	Non-Init	Total	
Event Type↓							
Loss of Electric Power	7	0	7	1	2	3	10
Loss RCS Inventory	2	3	5	0	2	2	7
Loss of RHR	7	7	14	2	3	5	19
ESF Actuation	2	0	2	0	0	0	2
Loss of EDG	0	0	0	0	1	1	1
TOTAL	18	10	28	3	8	11	39

Table B.2 Number of Initiator & Non-Initiator UACs & UAOs by Error Type

Error Type→	Mistakes			Slips			Unknown			Total
Error Kind→	Initiator	Non-Init	Total	Initiator	Non-Init	Total	Initiator	Non-Int	Total	
Error Mode↓										
UAC	10	7	17	8	3	11	0	0	0	28
UAO	0	7	7	2	0	2	1	1	2	11
Total	10	14	24	10	3	13	1	1	2	39

* UAC - Unsafe Actions of Commission
** UAO - Unsafe Actions of Omission

Table B.3 Number of Initiator & Non-Initiator UACs & UAOs by Location

Location→	In-Control Room			Ex-Control Room			Total
Error Kind→	Initiator	Non-Init	Total	Initiator	Non-Init	Total	
Error Mode↓							
UAC	6	3	9	12	7	19	28
UAO	0	2	2	3	6	9	11
Total	6	5	11	15	13	28	39

Table B.4 Number of Initiator & Non-Initiator UACs by Location for Error Type

Location→	In-Control Room			Ex-Control Room			Total
Error Kind→	Initiator	Non-Init	Total	Initiator	Non-Init	Total	
Error Type↓							
Slip	3	2	5	5	1	6	11
Mistakes	3	1	4	7	6	13	17
Total	6	3	9	12	7	19	28

Table B.5 Number of Initiator & Non-Initiator UACs by Location for Event Type

Location→	In-Control Room			Ex-Control Room			Total
Error Kind→	Initiator	Non-Init	Total	Initiator	Non-Init	Total	
Event Type↓							
Loss of Electric Power	1	0	1	6	0	6	7
Loss of RCS Inventory	1	0	1	1	3	4	5
Loss of RHR	3	3	6	4	4	8	14
ESF Actuation	1	0	1	1	0	1	2
Total	6	3	9	12	7	19	28

Table B.6 Number of Initiator & Non-Initiator UACs by Error Type for Event Type

Error Type→	Mistake			Slip			Total
Error Kind→	Initiator	Non-Initiator	Total	Initiator	Non-initiator	Total	
Event Type↓							
Loss of Electric Power	3	0	3	4	0	4	7
Loss of RCS Inventory	2	2	4	0	1	1	5
Loss of RHR	4	5	9	3	2	5	14
ESF Actuation	1	0	1	1	0	1	2
Total	10	7	17	8	3	11	28

Table B.7 Number & Types of PSFs for UACs & UAOs by Location

Error Mode→	UAC			UAO			Total
Location→	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	
PSF Type↓							
Communications	1	4	5	0	1	1	6
Design	2	3	5	0	3	3	8
HMI	6	5	11	2	3	5	16
Procedures	8	11	19	2	6	8	27
Supervision	0	2	2	0	0	0	2
Training	3	6	9	0	1	1	10
Other	0	1	1	0	0	0	1
Total	20	32	52	4	14	18	70

Table B.8 Number & Types of PSFs for Initiator & Non-Initiator UACs by Location

Error Kind→	Initiator			Non-Initiater			Total
Location→	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	
PSF Type↓							
Communications	1	3	4	0	1	1	5
Design	0	1	1	0	2	2	3
HMI	5	3	8	3	2	5	13
Procedures	6	8	14	2	3	5	19
Supervision	0	2	2	0	0	0	2
Training	2	4	6	1	1	2	8
Other	0	1	1	0	0	0	1
Total	14	22	36	6	9	15	51

Table B.9 Number & Types of PSFs for Initiator & Non-Initiator UACs by Error Type

Error Kind→	Initiator			Non-Initiator			Total
Error Type→	Mistake	Slip	Total	Mistake	Slip	Total	
PSF Type↓							
Communications	3	1	4	1	0	1	5
Design	0	1	1	2	0	2	3
HMI	4	4	8	2	3	5	13
Procedures	8	6	14	3	2	5	19
Supervision & 1 other	2	1	3	0	0	0	3
Training	2	4	6	2	0	2	8
Total	19	17	36	10	5	15	51

Table B.10 Number of Initiator In-Control Room & Ex-Control Room UACs by Activity for Error Type

Activity Type→	Maintenance			Testing			Operations			Others			Total
Location→	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	
Error Type↓													
Slip	1	1	2	1	2	3	1	1	2	0	1	1	8
Mistakes	1	0	1	0	5	5	2	2	4	0	0	0	10
Total	2	1	3	1	7	8	3	3	6	0	1	1	18

Table B.11 Number of Non-Initiator In-Control Room & Ex-Control Room UACs by Activity for Error Type

Activity Type→	Maintenance			Testing			Operations			Other			Total
Location→	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	
Error Type↓													
Slip	0	0	0	0	0	0	2	1	3	0	0	0	3
Mistakes	0	0	0	0	2	2	1	3	4	0	1	1	7
Total	0	0	0	0	2	2	3	4	7	0	1	1	10

Table B.12 Number of In-Control Room & Ex-Control Room UACs by Activity for Event Type

Activity Type→	Maintenance			Testing			Operations			Other			Total
Location→	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	
Event Type↓													
Loss of EP	0	1	1	0	3	3	1	1	2	0	1	1	7
Loss of RCS Inventory	0	0	0	0	1	1	1	2	3	0	1	1	5
Loss of RHR	1	0	1	1	4	5	4	4	8	0	0	0	14
ESF Actuation	1	0	1	0	1	1	0	0	0	0	0	0	2
Total	2	1	3	1	9	10	6	7	13	0	2	2	28

Table B.13 Number of Initiator In-Control Room & Ex-Control Room UACs by Personnel Type for Error Type

Personal Type→	Licensed-Operators			Non-Licensed-Operators			Technicians			Contractors			Total
Location→	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	
Error Type↓													
Slip	2	0	2	0	0	0	1	2	3	0	3	3	8
Mistakes	2	0	2	0	2	2	1	4	5	0	1	1	10
Total	4	0	4	0	2	2	2	6	8	0	4	4	18

Table B.14 Number of Non-Initiator In-Control Room & Ex-Control Room UACs by Personnel Type for Error Type

Personal Type→	Licensed-Operator			Non-Licensed-Operator			Technicians			Contractors			Total
Location→	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	
Error Type↓													
Slip	2	0	2	0	1	1	0	1	1	0	0	0	4
Mistakes	1	0	1	0	0	0	0	0	0	0	5	5	6
Total	3	0	3	0	1	1	0	1	1	0	5	5	10

Table B.15 Number of In-Control Room & Ex-Control Room UACs by Personnel Type for Event Type

Personal Type→	Licensed-Operators			Non-Licensed-Operators			Technicians			Contractors			Total
Location→	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	In-CR	Ex-CR	Total	
Event Type↓													
Loss Electric Power	1	0	1	0	1	1	0	4	4	0	1	1	7
Loss of RCS Inventory	1	0	1	0	0	0	0	1	1	0	3	3	5
Loss of RHR	5	0	5	0	2	2	1	1	2	0	5	5	14
ESF Actuation	0	0	0	0	0	0	1	1	2	0	0	0	2
Total	7	0	7	0	3	3	2	7	9	0	9	9	28

Table B.16 Characteristics of Pre-Accident and Initiator Unsafe Acts

Event Identifier/Significant or Unusual Plant Conditions	Action*	PSFs**
Braidwood 1: (10/4/90) (Loss of RCS Inventory) • Planned breach of RCS pressure boundary • Two procedures performed simultaneously	P: Did not wait for confirmation that RHR vent valve was closed	- Procedures - Stress - Communications (3) - Organizational factors
	I: Drain-path created by opening RHR hot leg suction valve	- Procedures - Stress - Communications (2) - Organizational factors
Prairie Island 2: (2/20/92) (Loss of RHR) • Planned RCS draindown • N_2 pressure higher than normal • Inexperienced draindown crew	P: Errors in RV level determination	- Human-System interface - Procedures (2) - Supervision - Training - Communication - Instrumentation
	P: Inadequate N_2 pressure control	- Procedures - Training
	I: Overdraining of RCS	- Human-System interface - Procedures (2) - Supervision - Training - Communication - Instrumentation
Oconee 3: (3/8/91) (Loss of RCS Inventory) • Planned breach of RCS pressure boundary	P: Blind flange on wrong LPI sump line	- Human-System interface - Procedures - Training (2) - Organizational factors (2)
	P: Independent checking failed	- Human-System interface - Procedures - Training - Organizational factors
	I: RCS drain-path through unblanked line	- Organizational factors - Procedures - Communications

*P = Pre-accident unsafe act, I = Initiating unsafe act

** (#) = number of multiple effects for same PSF category

Table B.16 Characteristics of Pre-Accident and Initiator Unsafe Acts

Event Identifier/Significant or Unusual Plant Conditions	Action*	PSFs**
Braidwood 1: (10/4/90) (Loss of RCS Inventory) • Planned breach of RCS pressure boundary • Two procedures performed simultaneously	P: Did not wait for confirmation that RHR vent valve was closed	- Procedures - Stress - Communications (3) - Organizational factors
	I: Drain-path created by opening RHR hot leg suction valve	- Procedures - Stress - Communications (2) - Organizational factors
Prairie Island 2: (2/20/92) (Loss of RHR) • Planned RCS draindown • N_2 pressure higher than normal • Inexperienced draindown crew	P: Errors in RV level determination	- Human-System interface - Procedures (2) - Supervision - Training - Communication - Instrumentation
	P: Inadequate N_2 pressure control	- Procedures - Training
	I: Overdraining of RCS	- Human-System interface - Procedures (2) - Supervision - Training - Communication - Instrumentation
Oconee 3: (3/8/91) (Loss of RCS Inventory) • Planned breach of RCS pressure boundary	P: Blind flange on wrong LPI sump line	- Human-System interface - Procedures - Training (2) - Organizational factors (2)
	P: Independent checking failed	- Human-System interface - Procedures - Training - Organizational factors
	I: RCS drain-path through unblanked line	- Organizational factors - Procedures - Communications

*P = Pre-accident unsafe act, I = Initiating unsafe act

** (#) = number of multiple effects for same PSF category

Table B.17 Characteristics of Post-Accident Actions

Event/Significant Conditions	Action*	PSFs**	Cues for Diagnosis		
			Misleading	Discounted	Used & Useful
Braidwood 1: (10/4/90) (Loss of RCS Inventory) Planned breach of RCS pressure boundary.	P: RCS drainpath isolated	+ Communications			• Phone call to CR re: RCS breach
Prairie Island 2: (2/20/92) (Loss of RHR) Planned breach in RCS pressure boundary.	P: Refill RCS & restore SDC	+ Procedures + Supervision + Instrumentation			• Electronic level indication (came on scale) • RHR pump low flow, low suction pressure & low motor-amp current alarms
Oconee 3: (3/8/91) (Loss of RCS Inventory) Planned breach in RCS pressure boundary.	Sub: Opened BWST suction isolation valves before isolating drainpath to sump	- Instrumentation + Procedure + Communications + Instrumentation	• Reactor building normal sump high-level alarm • RV level decreasing	• Reactor building emergency sump high-level alarm	• RV ultrasonic level alarm • Report from containment re: decreasing RV level & increasing radiation • LPI pump A current fluctuating downward
	P: Isolate drainpath (& closed BWST isolation valves) & refill RCS	+ Instrumentation			• RV level indication
Crystal River 3: (12/8/91) (Loss of RCS Pressure Transient) Startup/transition in power.	Sub: Increased RX power before knowing reason for RCS pressure decrease Sub: Bypassed ESFAS before knowing reason for RCS pressure decrease	+ Instrumentation - Instrumentation - Procedures	• PZR spray valve indication (shows closed even though valve is open) • Report re: steam flow to deaerating feed tank	• PZR level increasing • RCS temperature decreasing	• RCS pressure decreasing • RV level, sump levels, radiation monitors (i.e., no LOCA) • S/F & feedrates normal
	P: Close PZR spray valve & control RCS pressure	+ Instrumentation - Procedures and/or training			• RCS pressure trends • PZR vapor space temperature trends
Braidwood 1: (12/1/89) (Loss of RCS Inventory) Preparing to enter hot shutdown from cold shutdown (i.e., drawing PZR bubble & increasing RCS pressure)	Sub: Isolated operating RHR B train	+ Instrumentation + Communications - Procedures + Training - Training	• Report of leak in vicinity of RHR A relief valve		• Containment parameters (pressure, humidity, temperature, sump levels) (i.e., not in containment) • PZR level, RHR pump motor current • Reports on holdup tank level increase • RCS pressure decreasing
	P: Isolated RHR A train (w/ open RV) & restored PZR level	+ Training + Communications + Instrumentation			• Report of flow through RHR B relief valve • PZR level & RCS pressure trends

*P = Successful post-accident action; Sub = Sub-optimal, intermediate action

** - indicates a positive PSF effect
+ indicates a negative PSF effect

B.6 REFERENCES

1. Barriere, M.T, Luckas, W.J., Whitehead, D.W., et. al., *An Analysis of Operational Experience During Low Power and Shutdown and A Plan for Addressing Human Reliability Assessment Issues*, NUREG/CR-6093, Upton, NY: Brookhaven National Laboratory, and Albuquerque, NM: Sandia National Laboratories, February 1994.

2. Luckas, W.J., Wreathall, J., Cooper, S.E., Barriere, M.T., and Brown. W.S., Human Reliability Influences During Low Power and Shutdown Conditions in PWR Nuclear Power Plants, Appendix C of NUREG/CR-6093, Upton, NY: Brookhaven National Laboratory, August 1992.

3. Whitehead, D.W., Forester, J., Parry, G.W., Haas, P.M., and Donovan, M., Human Reliability Influences During Low Power and Shutdown Conditions in BWR Nuclear Power Plants, Appendix B of NUREG/CR-6093, Albuquerque, NM: Sandia National Laboratories, October 1992.

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

5. Harbour, J., *On-Site Investigation and Analysis of the Human Factors of an Event at Braidwood Unit 1 on October 4, 1990 (Reactor Coolant System Loss)*, Idaho Falls, ID: Idaho National Engineering Laboratory, October 1990.

6. Steinke, W., Hill, S., Meyer, O. and Kauffman, J., *Trip Report: Onsite Analysis of the Human Factors of an Event at Prairie Island Unit 2, February 20, 1992, Loss of (Residual Heat Removal) Shutdown Cooling*, EGG-HFRU-10228, Idaho Falls, ID: Idaho National Engineering Laboratory, April 1992.

7. Meyer, O., *Trip Report: Onsite Analysis of the Human Factors of an Event at Oconee Unit 3, March 8, 1991*, EGG-HFRU-9702, Idaho Falls, ID: Idaho National Engineering Laboratory, May 1991.

8. Meyer, O., *Trip Report: Onsite Analysis of the Human Factors of an Event at Crystal River Unit 3, December 8, 1991 (Pressurizer Spray Vale Failure)*, EGG-HFRU-10085, Idaho Falls, ID: Idaho National Engineering Laboratory, January 1992.

9. *Augmented Inspection Team Report: Inspection on December 2-4, 1989 of Braidwood Unit 1, Residual Heat Removal System, Train B,* Suction Relief Valve Event on December 1, 1989, Report No. 50-456/89030, Glen Ellen, Illinois: U.S. Nuclear Regulatory Commission, Region III, December 1989.

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

11. Personnel communications by Dennis Bley, Detailed HRA Project Working Meeting, December 13, 1993.

12. *Probabilistic Risk Assessment (PRA) Procedures Guide,* NUREG/CR-2300, Volumes 1 and 2, Washington, DC: U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, January 1983.

APPENDIX C

DEVELOPING AN APPROACH TO DEAL WITH HUMAN DEPENDENCY

(FIN L-2415, Task 8)

J. Wreathall, M.T. Barriere, S.E. Cooper,
D.C. Bley, and W.J. Luckas, Jr.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

C.1 INTRODUCTION AND CONCEPTS

This report describes work accomplished under Task 8 (Development of an Approach for Dependent Human Events) of the Improved PRA development program. The purpose was to examine the concern, identified in earlier tasks, that the level of dependency modeling implemented in typical commercial nuclear power plant (NPP) probabilistic risk assessments (PRAs) is not consistent with the experience observed in significant operational events. If the two are inconsistent, then this task should indicate directions for developing new modeling and quantification techniques for PRAs to be elaborated in subsequent tasks, particularly Task 10 (Development of Quantification Process), and Task 15 (Development of Implementation Guidelines).

Section C.1 identifies the underlying principles associated with considering dependencies between human failures in power plants and discusses these within the context of the framework developed in Task 6. Section C.2 examines the implications of these principles, with reference to the human-factors aspects found in practice. Section C.3 examines the operational experience for several significant operational events that were reviewed as part of the earlier Human Action Classification Scheme (HACS) evaluations. Finally, Section C.4 discusses the implications of the work, and how this relates to future project tasks.

C.1.1 Definitions

Simply stated for this task, a dependency is the property of two or more basic PRA events (a, b) involving unsafe or recovery actions that cause the following probabilistic relationship to be true:

$$P(a,b) \neq P(a)\,P(b)$$

In most cases, the dependence mechanisms of concern are those that influence multiple human actions in the same PRA cut-set. The various kinds of dependence mechanism that can cause this are discussed next.

C.1.2 Examples of Dependencies

Figure C.1 indicates the differences in the analysis of dependencies between that typically taken in PRAs of commercial NPPs, and the experience found in our analyses of data. Figure C.1 demonstrates a range of possible time-phases for dependency influences to act. These could be between any combinations of pre-initiating event, initiating event, post-initiating event, and recovery actions. In addition, multiple dependent human errors could occur within any of those individual time phases.

The following are examples of dependencies influencing multiple human actions potentially important in PRAs:

- direct dependence on some common process external to the tasks being performed (e.g., procedure-writing or planning);
- multiple interdependent actions in response to a single rule-based mistake (e.g., misdiagnosis);
- task-sequential, single-person (or group) dependencies -- errors in performing Task A influences reliability of subsequent Task B;

- multiple tasks involving common PSFs, such as common supervision or a common procedure;
- direct task interactions, such as failure in Task A causing failure in Task B (e.g., error in calibrating level sensors causing incorrect measurement of levels, which causes the operation of mitigating systems to fail), and
- tasks having indirect "knock-on" effects by changing the plant's conditions in unplanned way such as changing timescales, patterns of symptoms, or creating new opportunities for errors.

The data analyses performed earlier in Task 6 (Appendix A) indicate that the most frequent combination of multiple unsafe acts was combinations of active and latent failures, most frequently occurring as pre-accident latent failures and initiating active failures. The second most common combination was initiating active failures followed by post-accident active failures.

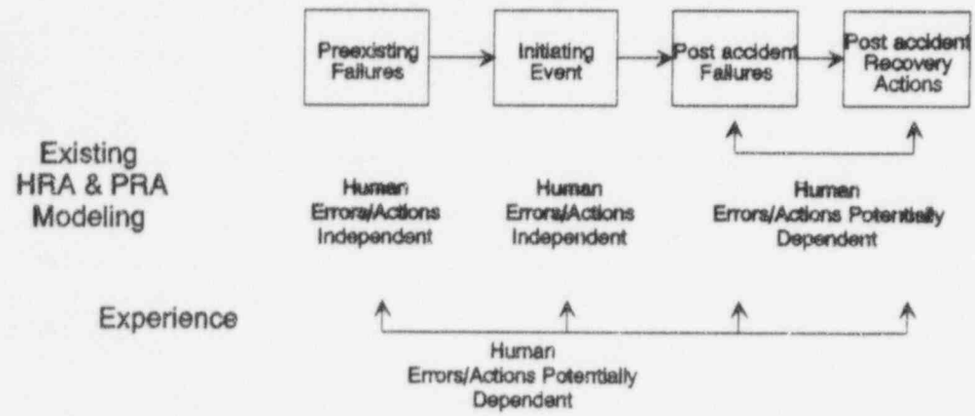
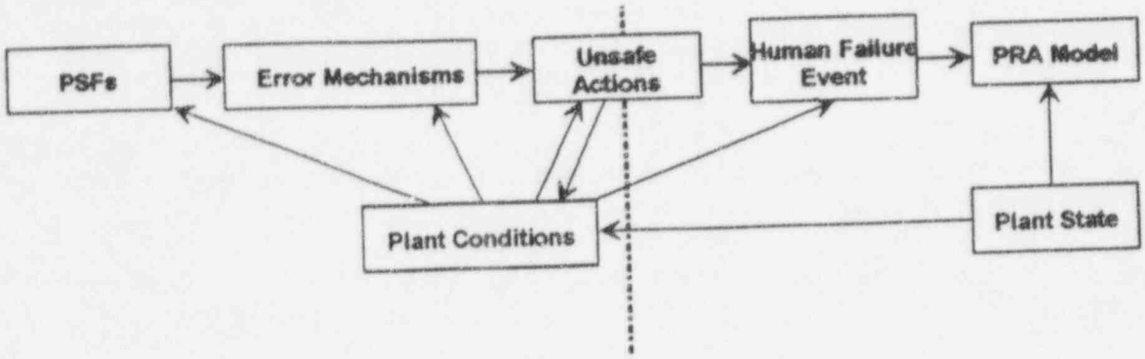


Figure C.1 Differences between typical PRA dependence modeling and actual events

C.1.3 Framework for Identification of Dependencies

As discussed in Appendix A, Task 6 developed a framework that describes how unsafe acts can contribute to degradations in safety and that their interrelationships should be modeled in PRAs. The framework as shown in Figure C.2, is divided into several elements including: performance shaping factors (PSFs), error mechanisms, unsafe actions, plant conditions, and human failure events. PSFs and plant conditions play critical roles in influencing the occurrence and form of error mechanisms. Unsafe actions are intermediate manifestations of errors. Human failure events are associated with breached defenses or initiating events as represented in PRAs.

The two primary causal groups for unsafe actions, PSFs and plant conditions, have the potential for originating in common (organizational) processes. For example, an ineffective procedure-development or training program could lead to deficiencies in those PSFs for several groups involved in numerous plant activities. Similarly, poor planning could allow multiple activities to be performed simultaneously, which can create an unanalyzed plant condition. Catalogs of organizational processes have been developed in research programs associated with organizational processes, such as those performed by Brookhaven National Laboratory,[1] the University of California at Los Angeles (UCLA),[2] the University of Minnesota,[3] Science Applications International Corporation (SAIC),[4] and others.



HRA, Human Factors, Behaviorial Science, & Plant Engineering

PRA

Figure C.2 Multidisciplinary HRA framework

Figure C.3 shows how these influences, i.e., plant conditions and performance shaping factors (shown in Figure C.2) and the common processes can combine to create one of the most common cases of multiple unsafe actions, those of an active and a latent failure, such as a failed mitigating system combined with an initiating event. Examples of such processes are illustrated in the figure.

(We note here that the framework developed in this project (see Appendix A) continues to evolve, partly because issues requiring consideration continue to emerge, and are expected to do so throughout the rest of this project. It is intended that the following discussions are consistent with the earlier development. However, shades of differences may emerge in the interpretation of the elements in the framework. At a later stage, we intend to reconcile and unify such differences, but, this is not expected to be completed until later in the quantification development task (Task 10.)

C.1.3.1 Performance Shaping Factors (PSFs)

The PSFs are those influences that determine the reliability of the task as designed. These factors include, the human-machine interface design in the control room or any other work area, the useability of the procedures, communications, and training, as well as organizational attributes. PSFs were selected as part of creating the HACS database, as discussed in Reference 5.

C.1.3.2 Plant Conditions

Plant conditions are the factors that influence the potential for unsafe actions in a particular work setting and include the configuration of equipment, the provision and operability of plant instrumentation and data systems, and the plant evolutions (activities) taking place. The plant conditions have the potential to act as common influences on all tasks being performed in a period. For example, essential equipment normally required as part of plant technical specifications may be unavailable or realigned to non-normal electrical or inventory sources. As a result, actions taken involving these sources could produce unusual consequences if the systems are required for some other activity related to current plant conditions. In turn, recovery could be delayed or made more complex.

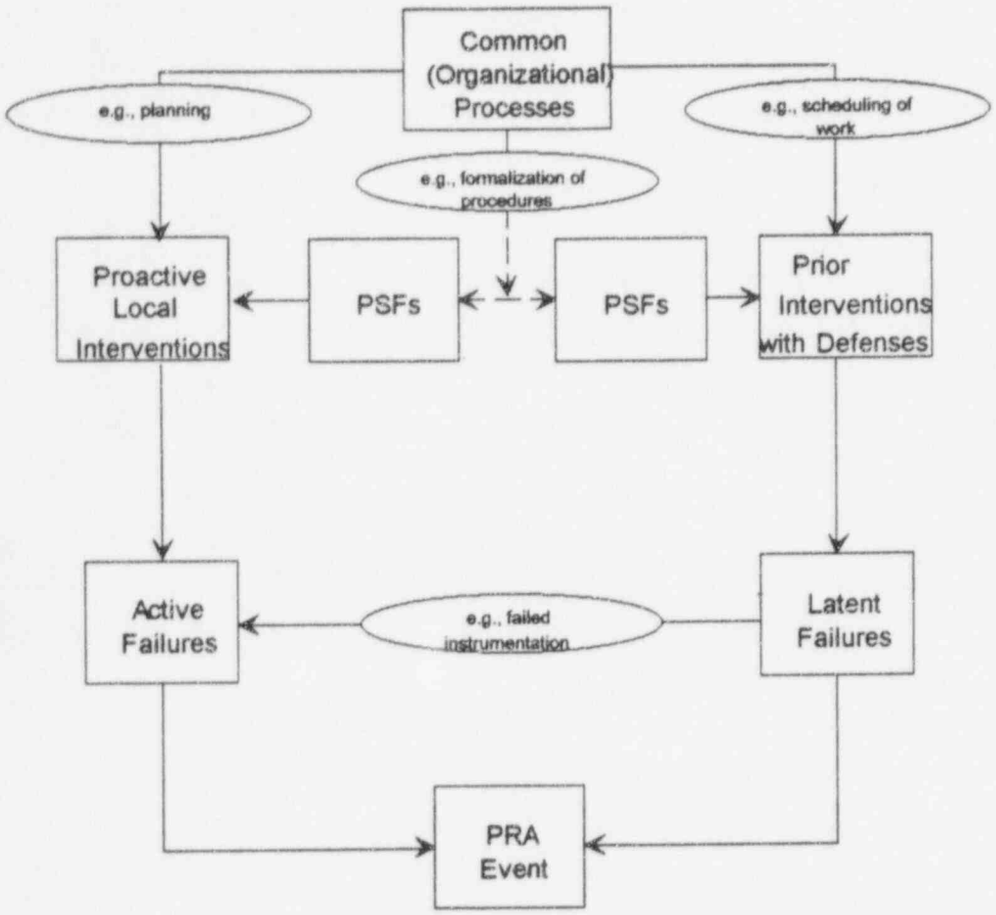


Figure C.3 Potential pathways for multiple dependent events

C.1.3.3 Common Processes

Common organizational processes, or, more simply, common processes are those programmatic activities carried out in several parts of the plant that have the potential to influence different groups, possibly at different times, carrying out different kinds of tasks. Examples would include programs associated with planning, training, and developing procedures.

These programs often are set up within the plant or corporation as a common activity. Therefore, a deficiency in the program can spread the potential for poor practices or create problem situations throughout the plant. For example, consider inadequate planning for an outage. With reference to Figure C.3, the effects of inadequate planning could result in work being scheduled on a train of an emergency power system that makes the equipment unavailable (prior intervention with defenses), while, at the same time, scheduling upgrading work on the one incoming unit supply. Hence the likelihood of a unit blackout is increased.

More directly related to human performance are those cases where the common processes can create deficiencies in the PSFs, such as procedures, instrumentation, or even knowledge of plant vulnerabilities. For example, the process of developing procedures could create several that have a less-than-adequate

technical review and contain assumptions or directions that do not reflect the plant as operated (for example, during outages). Procedures with these flaws then could be sent to both operations and maintenance for tasks during the outage. In turn, these can create human failures associated both with interventions with defenses and active tasks, consequently creating initiating events and flawed responses.

C.1.3.4 Interventions with Defenses, Barriers, and Safeguards

Measures aimed at preventing, mitigating, or protecting against hazards represent an extensive part of the facilities of a nuclear power plant; these generally include the emergency core cooling systems (ECCS) and other related equipment during normal operations. However, during LP&S operations, other defensive measures and the Reactor Coolant System (RCS) itself become important. ECCS equipment often is taken out of service for maintenance or is no longer appropriate for plant conditions during outages. The RCS volume and boundary are deliberately changed. Therefore, the interactions by people with all the systems that prevent, mitigate, or protect against hazards must be considered.

These defenses, barriers, and safeguards can be classified along two relatively independent dimensions: (a) the functions served, and (b) modes of application within an organization.

Functions

- To create awareness and understanding of the risks and hazards.
- To detect and warn of the presence of off-normal conditions or imminent dangers.
- To protect people and the environment from injury and damage.
- To recover from off-normal conditions and to restore the system to a safe state.
- To contain the accidental release of harmful energy or substances.
- To enable the potential victims to escape out-of-control hazards.

Modes of Application

- Engineered safety features (e.g., automatic scram and ECCS systems)
- Policies, standards, and controls, such as technical specifications (administrative and managerial measures designed to promote standardized and safe working practices that together constitute the "safety management system").
- Procedures, instructions, and supervision (measures aimed at providing local task-related knowledge).
- Training, briefing, drills (providing and consolidating safety awareness and safety knowledge).
- Personal protective equipment (anything from overshoes to breathing suits).

Figure C.3 shows that latent failures can result from deficiencies in human involvement at an early stage with these systems that renders them ineffective at the time of an initiating event, which is, itself, the result of an active unsafe action.

In addition, the earlier latent failure can cause a subsequent active failure. Perhaps, this is most noticeable where the latent failure involves instrumentation, especially instrumentation for reading the level in the reactor coolant system (RCS) during reactor draindown. Its failure causes the operators to over-drain the vessel, which frequently leads to loss of the capability to remove decay heat. Several such events are discussed in Section C.3.

C.1.4 Types of Dependence Causal Mechanisms

Figure C.3 presents a way for discussing dependence mechanisms between active and latent failures leading to the following proposed classification.

The active- and latent-failure paths may originate from (i.e., depend on) a set of *common processes*. These common processes are activities within the organization, such as planning, developing procedures scheduling, that fundamentally influence all plant-wide activities important to safety. These can be considered specific common-cause mechanisms. During an outage, such a common process could lead to the scheduling of maintenance on a component without ensuring alternative equipment is available (a latent failure involving a loss of a defense). For example, if the RCS level instruments were replaced during draindown of the RCS level to midloop, then the probability is much increased of an operator making an active error leading to inadvertent excessive draindown and loss of core cooling.

However, not all dependencies result directly from these common processes. There can be cases where *common performance shaping factors (PSFs)* may influence the probabilities of occurrence for multiple unsafe acts. Simple examples would include the workplace environment (heat, light, displays, and so on), and procedures and training; factors directly related to humans could include: "ownership" of the plant, morale, motivation, technical knowledge, skills and abilities, and local peer work norms (important for circumventions).

In addition to the common PSFs, *plant conditions* could result in levels of dependence between multiple unsafe acts; these include timing between events (e.g., one event masks or coincides with another), the rates of change in plant parameters, and the inherent hazards associated with unique plant evolutions. For example, the hazards associated with partial draining of the RCS are much greater shortly after a reactor trip (when the decay heat is high) than after an extended period. Because of the nature of this hazard, unsafe actions that normally would be considered independent because there is adequate time for operators to diagnose and correct each of them now compete with each other in terms of such resources. For instance, in one event where RCS overdraining occurred within 48 hours of the shutdown, operators only had a time window of about 20 minutes to diagnose and correct all failures associated with loss of residual heat removal (RHR).

Finally, there can be cases where *one failure causes another*, particularly when one of them changes the plant conditions in subtle or hidden ways. For example, a latent failure could occur when calibrating level measurements; the miscalibrated instrument leads an operator to over-drain the reactor vessel. If the calibration task is being performed concurrently with the draining operation, the miscalibration has changed the plant conditions from the initial set when the instrumentation was operable and accurate.

C.2 REVIEW OF CAUSES OF DEPENDENT EVENTS

The purpose of this section is to review experience of the causes of dependent events, defined in Section C.1. Each of the categories of causes will be reviewed in turn. Discussion of the kinds of interventions found important in the Human Action Classification Scheme (HACS) database are included in Section C.3. To help in this review, examples of dependency causes are quoted from one of the significant operational events reviewed, the March 8, 1991, event at Oconee, Unit 3.[6] Table C.1 summarizes the event in terms of the multidisciplinary framework and the related dependence mechanisms discussed in Section C.1.

C.2.1 Common Performance Shaping Factors (PSFs)

The category of common PSFs relates to the potential effects of such influences as a common procedure, a common human-systems interface, and a common training program. If these are less than adequate, they have the potential, of causing a significant increase in the probabilities of failures for all those actions affected by them.

Table C.1 summarizes one example from the event at Oconee. There, a sequence of errors occurred that were largely (though not exclusively) the result of several operators separately being misled by an erroneous label. That label used, not the formal plant label which was very difficult to see, directed the operator to the wrong train and misled both the operators installing the blind flange and different operators later checking the installation.

The second example of a common PSF was the deficiency in training that was reflected by a lack of questioning attitudes to earlier work. Standard operating practices, such as rechecking the configuration before opening a potential RCS drain path normally are part of the training program. However, in this event the operators did not, recheck before opening the isolation valve. This failure, together with the failure to detect the incorrect installation by the checking crew, reflects a lack of training in standard operating practices.

C.2.2 Common Processes

Common processes are those that, are common-mode influences to whole groups of human actions. They include senior management decisions, work organization and planning, procedure and training development, and other programmatic functions within the plant or utility. Deficiencies in these processes can lead to poor or erroneous performance simultaneously in most plant departments, and between work teams within departments. One simple example would be the case where a lack of work planning led to the simultaneous maintenance of two redundant trains of diesel generators during a refueling outage. A second would be the development of technically inaccurate procedures (within the procedure development process), that led to errors in performance by both operations and maintenance workers.

Table C.1 gives the common processes which were influences in the 1991 Oconee Unit 3 event. First, there were common deficiencies in the written instructions (procedures and work orders) about the formal identification of equipment. Neither the work instructions nor the procedures used to check the work formally identified the specific penetration number, resulting in two groups of operators separately using

informal markings as the basis for identification. Second, the procedures had no requirement on the part of the final group of operators to confirm or recheck that the blind flange was correctly installed before effectively opening an un-isolated RCS drain path. This combination of deficiencies is an initial indication that the plant's procedure development program was deficient at that time.

Table C.1 Summary Analysis of March 1991 Oconee Unit 3 Event

Plant Conditions:		
- Day 24 after refueling		
- No measurements of RCS vessel or loop temperature		
- Containment closed but rad monitors inoperative		
Unsafe Actions:	**PSFs:**	
	Unsafe Action(s)	PSF
1. Blind flange for RHR suction line installed on wrong line - EOC, latent, RB mistake (instructions, label)	(1)	Incorrect use of drawings
	(1)	Procedure did not identify penetration ID #
2. Subsequent checking failed to detect error - EOO, latent, RB mistake (label)	(1,2)	Incorrect informal label
	(1,2)	Poor visibility of formal label
3. RCS drained by operators through unblanked line - EOC, active, KB mistake (no final check by ops, failure to control plant configuration by LO, pursued wrong causes by NLO action)	(3)	Poor communications between maintenance and control room
	(3)	Procedure did not specify coordination between maintenance and operations
	(3)	Lack of task awareness by operations
Dependencies:		
Unsafe Actions	Dependence Mechanisms	
(1-2)	**Common PSFs** - labeling, visibility, organizational processes: control of workspace	
(2-3)	**Common PSFs** - training: unquestioning reliance on prior procedural actions, no double checks (Note: latent failure in (2) set up (3) - temporal)	
(2-3)	**Common (Organizational) Processes** - unquestioning reliance on quality of prior work	
(1,2-3)	**Common (Organizational) Processes** - deficient instructions/procedures: penetration identification # not defined (1) & no requirements for recheck (3)	

In addition, the lack of any true independent checking by the second group of operators and by the operators immediately before they opened the isolation valves indicated a common over-reliance on work performed previously. There seemed to be no analysis of how the penetration could not have been isolated by the blind flange, and therefore, what steps were required to confirm that the installation was correct, either by the operator "checker" or the test crew. These actions were well separated in time (several days from start to finish). Rather than being associated with specific PSFs or the local factors

such as common supervision, these errors indicate a common organizational process that tolerated the use of informal markings and an over-reliance on the quality of previous work.

To develop an improved HRA methodology, there needs to be increased sensitivity to issues that have been found in the data reviews. To make progress in evaluating common processes, work on the influence of common (organizational or other) processes on safety will be reviewed. Then, HACS data and other sources will be searched to identify the degree to which these common processes were significant human performance influences in the events reviewed. In particular, the applicability of three approaches will be considered.

The first approach, developed at BNL and reported in Barriere, et al.,[7] is a systematic approach for evaluating quantitatively the influence of organizational factors on estimates of human error probabilities (HEPs). This is accomplished primarily through incorporating organizational factors, in general, into upper and lower HEP uncertainty bounds. These bounds establish a "bandwidth" in which revised HEP estimates are calculated using plant-specific organizational factors. This approach could be expanded to assess the effects on HEP estimates of a number of PSFs, such as human-system interfaces, procedures, and training.

The second approach, developed at the University of California at Los Angeles (UCLA) and reported in Davoudian et al.[2] involves work-process analyses, which evaluate how common organizational processes influence specific task-related PSFs. Methods that have followed this approach seem to face the difficulty in considering large numbers (20 or so) of organizational dimensions (e.g., common processes) interacting with a comparable number of task factors. Assessing the resulting large numbers of combinations leads difficulties in the ranking and weighting process since almost all organization dimensions potentially interact with almost all local task factors. Simplifications to reduce the numbers of ratings are being considered. This approach would be simplified by reviewing HACS data and other evidence of the more important combinations. A significantly smaller number of factors (both organizational and local) would probably be sufficient to describe most events.

The third approach is that used in the chemical process industries to assess the influence of organizational factors on safety. Several methods are used, most of which are proprietary to individual consulting companies. One such example is the MANAGER assessment system.[8] In this auditing-based method, questionnaires are used to evaluate what are effectively performance indicators associated with specific plant departments, such as operations and maintenance. Indices associated with the "quality" of these departments then are developed to provide a score relative to industry norms. Then; depending on that relative ranking, the numerical results of the PRA are modified based on assumed distributions of the effects of plant norms. In other words, where a plant is rated "10 times better" than the average, the assessed level of risk is adjusted accordingly. This, and other similar methods are in constant states of revision, building on improved data. For example, data assessing the effects of management on failure rates of equipment were reported recently,[9] using data gathered under sponsorship of the U.K. Health & Safety Executive.

C.2.3 Plant Conditions

In addition to the common processes and the common PSFs, plant conditions are an important factor in creating the potential for dependent failures. They create the environment within which the work is being performed, which can have a significant influence on all the tasks. Perhaps the broadest view of plant conditions during low-power and shutdown operations is that many systems and features are not available

that are taken for granted during full-power operations. For instance, the plant may have only one incoming electrical supply and normal instrumentation may be disconnected or non-operational, with operators having to rely on temporary measuring systems (as with level sensing at midloop at many PWRs). For most plants, limiting conditions of operation associated with the availability of equipment do not exist during outages. In addition, operators and other plant personnel are making many more manual interventions with the plant, so there are many more opportunities for errors of commission or other errors that create unusual failure modes, which in turn, create new opportunities for error because of the previously unplanned conditions.

Beyond these very general aspects of plant conditions are the more direct task-relevant plant conditions. For example, the failures or deficiencies of temporarily installed level instrumentation played a significant role in several events as discussed in several evaluations of low-power and shutdown events, including NRC's NUREG-1449.[10] (This particular plant condition is considered different from the PSF of human-system interface because the condition of the plant that renders the instruments deficient; the ergonomic aspects of the instrumentation system are not at fault.) System failures of instrumentation have the potential to cause multiple unsafe actions because they create a false perception in the minds of the operators about the condition of the plant. This can cause operators to take inappropriate actions, which also can create difficulties in recovering from them.

C.3 ANALYSIS OF DEPENDENCIES IN EVENT DATA FROM A PRA PERSPECTIVE

The approach to incorporating dependencies, in common with the other tasks in this development program, is strongly influenced by the experiences observed in actual events occurring during low-power and shutdown events. To develop this approach, full-text LER events in the HACS database and those reported in the AIT or AEOD human factors study reports involving multiple unsafe actions were "re-reviewed" to identify the kinds of events involving multiple unsafe actions, the extent to which these would be incorporated as multiple human failure events in PRAs, and any causes of dependencies required in PRA modeling.

C.3.1 Review of Full-Text LER Events

Seven full-text licensee event reports (LERs) contained in the HACS database were initially identified as involving multiple unsafe actions (described in Attachment CA). On review, two of the seven events were found not to involve multiple human failure events, and the remaining five events each involved two human failure events. In each of the latter, there was no evidence that indicated the presence of a dependence mechanism.

For example, in the February 1986 shutdown event at Crystal River Unit 3, the shaft on the one running residual (decay) heat removal (RHR) pump failed mechanically. Startup of the redundant RHR pump was delayed because the suction valve to that pump would not open. Subsequent investigation showed that both these failures were the result of separate unsafe actions. The failure of the pump shaft was caused by prolonged operation with some degree of air entrainment which resulted in fatigue failure; the air entrainment was caused by operators controlling the RCS water level below that needed to prevent air entrainment. The suction valve failed to open due to inadequate preventive maintenance, which left the drive shaft and coupling under-lubricated. The two unsafe actions (operating at low level and inadequate prevent maintenance) were separated in time, involved different departments within the plant, and did not involve any common PSFs. The LER did not identify any specific common processes or organizational programs associated with these two failures. (This event is described further in Attachment Subsection CA.1.1.)

Similar results were found for the other LERs describing multiple human failure events. Table C.2 identifies the actual events, the number of associated human failure events, and the findings on dependencies.

C.3.2 Review of AIT and AEOD Events

In addition to the full-text LER events, seven low-power and shutdown events (LP&S) were described in AIT and AEOD human factors study reports. (In two cases, the same event was described in both an AIT and an AEOD report.) In five of them, multiple human failure events were identified. In four events there were two human failure events, and in one event there were three human failure events. With one exception, dependence mechanisms were identified in these events. These four events with dependencies identified are described below. Summaries of those events not involving dependence mechanisms or only involving one human failure event (HFE) are contained in Attachment CA.2. Table C.3 summarizes all these events and the findings concerning dependencies.

Table C.2 Summary of Review for Dependency from Full-Text LERs

Location of Event Description in Attachment CA	Plant	Number of HFEs	Dependencies Identified
CA.1.1	Crystal Rr 3	2	None identified
CA.1.2	Arkansas 1	1	N/A
CA.1.3	Arkansas 2	2	Second failure caused by the first
CA.1.4	Waterford 3	1	N/A
CA.1.5	Shearon Harris	2	None identified
CA.1.6	Catawba 1	2	None identified
CA.1.7	Vogtle 1	2	None identified

Table C.3 Summary of Review for Dependency from AIT and AEOD Human Factors Study Reports

Location of Event Description in Attachment CA	Plant	Number of HFEs	Dependencies Identified
CA.2.1	Braidwood 1	2	Common process: procedures
CA.2.2	Diablo Can 1	2	Common PSFs: communications, org. factors
CA.2.3	Oconee 3	3	Common PSFs: procedures, org. factors
CA.2.4	Crystal Rr 3	2	Common PSF*
CA.2.5	Prairie Is 2	1	N/A
CA.2.6	Catawba 1	2	None identified
CA.2.7	Braidwood 1	1	N/A

* Note: No specific PSF type was identified from the Crystal River Event Report (See attachment CA.2.4)

C.4 IMPLICATIONS FOR MODELING OF DEPENDENT EVENTS

Section C.4.1 discusses the implications of how dependencies can be accommodated within PRAs. Incorporating the influence of common performance-shaping factors and their potential source, common processes, is discussed in Section C.4.2. The influence of plant conditions is discussed in Section C.4.3.

C.4.1 Level of Representation of Human Failure Events in PRAs

On the basis of the fourteen events identified in the previous section, the potential clearly exist for dependencies between basic events involving human actions. However, the potential perhaps is not as great as would be inferred from a simple review of the event reports (especially the AIT and AEOD events), where multiple unsafe actions were observed often with dependencies between them, but when reviewed from the PRA perspective, many of these multiple unsafe actions become condensed to a single human failure event. This is illustrated best by the 1992 Prairie Island Unit 2 event (Attachment Subsection CA.2.5) in which, numerous unsafe actions were made by different individuals, from misreading the temporary level measurements (the tygon tube level was almost inaccessible), to making errors in calculating dra. time (lack of precision in manipulating the data), and to the supervisors not monitoring the draindown activities. However, the outcome from the HFE perspective was an overdraining event with loss of RHR - an initiating event.

To what extent should PRAs be modified to reflect more explicitly the human performance at the "unsafe actions" level? Many of the unsafe actions described in the events reviewed were what Hudson[11] has called tokens, that is, specific unsafe actions unique to a single event that are almost certain never to recur. Changes in procedures, training, or instrumentation frequently will be implemented by the plant. In most cases, the plant conditions that created the opportunity for the event are unique and very unlikely to be repeated. Therefore, representing specific unsafe actions in the PRA process would be almost impossible because of the very large number of combinations that could occur, each with a very low probability of occurrence.

It is considered more practical (at least within the scope of this project) to continue to incorporate human failure events in the PRA process, as discussed in the Section C.3.2. However, the quantification process that will be developed in a later phase of this project must be able to include consideration of combinations of unsafe actions in defining scenarios for quantification. As presently intended, the quantification process will incorporate two distinct stages, the first being an evaluation of previous events (such as those in HACS, and other report databases) an identification of similar scenarios and to use those as a basis for bounding probability estimates. Developments in ways to extend the HACS database to support this approach also are being considered.

C.4.2 Influence of Common Performance Shaping Factors and Processes

Tables C.2 and C.3 summarized the findings for the events reviewed in terms of the number of PRA human failure events and the dependency mechanisms. It is noticeable that the events identified as having dependencies between the human failure events are all associated with those described in the AIT or AEOD human-factors reports. This could be because the events involving AIT or AEOD reports typically are more "interesting" and worthy of special investigation, or because these reports provide more detailed analyses of events, and therefore, underlying influences are more likely to be identified. The second reason is consistent with the findings in Reference 5, which concluded that the AIT and AEOD reports provide a greater level of detail for discerning dependence information.

Three approaches were developed for the modeling common processes, as discussed in Section C.2.2: the Human Error Probability (HEP) uncertainty method,[7] the work-process analysis method,[2] and the MANAGER[8] (or similar) method. Of these, only the MANAGER method is being implemented, though not in NPP PRAs. All these methods require further collection of data on organizational factors to provide empirical measures for determining their influence. In addition, using event data could limit consideration of only those combinations of organizational and local factors that were found important in those events in the database.

The MANAGER approach, already driven by field experience, has the potential benefit of not requiring methodological development. Some data have been reported on the effects of organizational processes. However, the actual workbooks for the assessment are proprietary. Additionally, the methodology has only been applied in the chemical process and petrochemical industries.

C.4.3 Plant Conditions

Plant conditions associated with shutdown and full-power operations are significantly different, as discussed in Section 4.1.3 of Ref. 5. In particular, for low-power events, plant conditions are constantly changing, usually as a result of manual interventions and actions. These actions set up the possibility of inappropriate unsafe actions resulting in errors of commission (EOPs), which then create new or more confused situations for further unsafe actions. In addition, rules concerning the availability of redundant equipment are often less stringent; hence, actions to recover the plant may be not as simple as for most full-power events. Finally, many temporary controls and measurement systems are in use which may not be the most accurate or responsive for the whole range of conditions faced by operators. This can lead to multiple errors caused by a misunderstanding of the plant conditions. Examples of these are discussed below.

In almost all cases, shutdown operations have permitted operations with significantly relaxed technical specifications requirements; this manifests itself in reduced availability of redundant core-cooling systems, electrical supply, and instrumentation. Similarly, shutdown operations involve many more manual interventions with the plant systems, which both increase the frequency of interventions and create the opportunities for EOCs (see Appendix B of this report, entitled "Identification and Representation of Errors of Commission").

In terms of unsafe actions, two principal aspects of plant conditions have played a significant role. The first is the influence of instrumentation, particularly RCS level instrumentation. Several events occurred in which the operators were misled by faulty or deficient RCS level data, though these did not always involve multiple human failure events as described in Attachment CA Subsections; these include: Arkansas Nuclear One Unit 2 (CA.1.3), Waterford Unit 3 (CA.1.4), Catawba Unit 1 (CA.1.6), and Prairie Island Unit 2 (CA.2.5). The Crystal River 3 event (CA.1.1) also may be the result of faulty level information over a prolonged period. In addition, incorrect indications were contributors in the RCS overpressurization event at Catawba Unit 1 (CA.2.6) and the loss of RCS pressure control at Crystal River Unit 3 (CA.2.4). Thus, in seven out of fourteen events, instrumentation played a significant role. The deficiencies with the instrumentation were not associated (in all but one case) with the ergonomic aspects, such as readability and functional grouping - factors that can be assessed by walk-throughs of control rooms. Rather the deficiencies were functional, such as the instruments being out-of-service without the operators' knowledge at Catawba Unit 1 (CA.2.6) and the indicating lamp switch being controlled by the motor actuator, not the actual valve position at Crystal River Unit 3 (CA.2.4).

Incorrect instrumentation readings may be one of the most significant influences on operator performance in that, these values are mostly taken as "true," and used as a basis for diagnoses, which are then acted upon. In several cases discussed earlier (for example, Arkansas Nuclear One Unit 2 and Waterford Unit 3), the recovery actions were delayed because of the initial misdiagnoses. Reason,[12] among others, observed the great difficulty people have in discarding an early misdiagnosis even when contrary data are available and observed. Therefore, recovery from any event involving a faulty instrumentation reading must be considered to be more time-consuming. Operators taking inappropriate actions because of their incorrect diagnosis must be considered as a possible error of commission (EOCs), as in bypassing the (Engineered Safeguards Features Actuation System (ESFAS) controls during the loss of RCS pressure at Crystal River Unit 3 (CA.2.4).

The second aspect of plant conditions is the reduction in coverage of plant rules typically embodied in technical specifications during full-power operations; this has the effect of allowing multiple activities on redundant systems or equipment not located in the same trains. From the human-error perspective, the simultaneous performance of tests or other operations may create hazardous conditions without each individual activity being the "cause" of the hazard. The loss of RCS inventory at Braidwood Unit 1 (CA.2.7) and the excessive draindown at Waterford Unit 3 (CA.1.4) were examples. While these are not strictly dependent events, hazards result from these combinations, and therefore the PRA needs to develop a search scheme for such combinations.

C.4.4 "Crude Rules" for Guidance in Assessing Multiple Human Failure Events

This section provides some simple rules as an initial basis for assessing the dependence between multiple human failure events in PRA models. These rules will be re-assessed as the HACS database is extended and the quantification methods developed in Task 10. These rules are basic, oversimple, and probably do no more than bound the potential for dependencies on the basis of the observed events.

- **Dependence between unsafe actions is the rule.** Independence requires that there is:

  - no common procedures,
  - no common hardware,
  - no common PSFs,
  - no common personnel,

  even if the actions are well separated in time. The sparse reporting of dependencies in the LERs is seen more as an omission in the reports than as an absence of dependencies in the events. Of the five AIT or AEOD reports identifying more than one human failure event, only one did not identify dependencies.

- **Any initiating event that is instrument-driven will have adverse effects in the recovery phase.** Numerous examples exist where a faulty or flawed instrumentation system induced operators to initiate an accident and limited their ability to diagnose the accident.

- **Operations that are not as planned, or as intended by the planners or supervisors ("cowboy" operations) degrade the ability of operators to terminate problems.** Such operations occur during LP&S operations, as in the case of the loss of RHR at Catawba (see Attachment CA Subsection CA.1.6).

C.5 REFERENCES

1. Haber, S.B., O'Brien, J.N., Metlay, D.S. and Crouch (Shurberg), D.A., *Influences of Organizational Factors on Performance Reliability* , NUREG/CR-5538, Brookhaven National Laboratory: Upton, NY, December 1991.

2. Davoudian, K., Wu, J. S., & Apostolakis, G., Incorporating Organizational Factors into Risk Assessment Through the Analysis of Work Processes, *Reliability Engineering and System Safety*, Los Angeles, CA: University of California at Los Angeles in press.

3. Nichols, M.I., *Organizational Factors Influencing Improvements in Nuclear Power Plants*, NUREG/CR-5705, University of Minnesota Strategic Management Center: Minneapolis, MN, April 1992.

4. Wreathall, J., *The Development and Evaluation of Programmatic Performance Indicators Associated with Maintenance at Nuclear Power Plants*, NUREG/CR-5436, Science Applications International Corporation, Dublin, OH, May 1990.

5. Barriere, M., Luckas, W., & Whitehead, D., *An Analysis of Operational Experience During Low Power and Shutdown & A Plan for Addressing Human Reliability Assessment Issues*, NUREG/CR-6093, Upton, NY: Brookhaven National Laboratory, and Albuquerque, NM: Sandia National Laboratories, 1994.

6. Meyer, O., *Trip Report: Onsite Analysis of the Human Factors of an Event at Oconee 3, March 8, 1991*, EGG-HFRU-9702, Idaho Falls, ID: Idaho National Engineering Laboratory, May 1991.

7. Barriere, M.T., Luckas, W.J., Stock, D.A., and Haber, S.B., *Incorporating Organizational Factors into Human Error Probability Estimation and Probabilistic Risk Assessment* (Draft), BNL Technical Report, Upton, NY: Brookhaven National Laboratory, January 1994.

8. Williams, J.C., The MANagement Assessment Guidelines in the Evaluation of Risk (MANAGER) Technique, in *Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM)*, New York: Elsevier, 1991.

9. Wright, M., Bellamy, L., & Cox, R.A., Recent Developments in Chemical Plant QRA, in *Health, Safety & Loss Prevention in the Oil, Chemical & Process Industries*, Oxford, U.K.: Butterworth-Heineman Ltd., 1993.

10. U.S. Nuclear Regulatory Commission, *Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States*, NUREG-1449, Washington, D.C., 1993.

11. Reason, J.T., The Contributions of Latent Human Failures to the Breakdown of Complex Systems, *Philosophical Transactions of the Royal Society*, Series B. 327: 475-484, London, 1990; Reason, J.T., *Human Error*, New York: Cambridge University Press, 1990.

12. Reason, J., *The Cognitive Worm at the Core of the TRC Apple* (Panel Discussion), Human Factors Society, Annual Meeting, Orlando, Florida, 1989.

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

ATTACHMENT C.A

REVIEW OF EVENT REPORTS FOR DEPENDENCIES BETWEEN HUMAN ERRORS

CONTENTS

C.A.1 REVIEW OF FULL-TEXT LICENSEE EVENT REPORTS (LERS)

C.A.1.1 Loss of Decay Heat Removal, Crystal River Unit 3, 2/2/86 (LER 302-86-003, Rev. 2)

In this event, two failures occurred, plus one incipient failure was found, during repairs to a reactor coolant pump. The first failure was the loss of one loop of decay heat removal when the pump shaft failed on the running decay heat pump (DHP). Failure of the shaft was believed to result from operating the pump with some degree of air entrainment (caused by a low water level in the reactor) causing a fatigue fracture.

Startup of the redundant loop was delayed for 24 minutes because the suction valve to the second decay heat pump would not open because of inadequate maintenance that had left the drive shaft and coupling under-lubricated, and the torque-switch and circuit-breaker trip settings too low. The incipient failure involved damage to the pipe-hanger resulting from water-hammer effects when refilling the system.

This event represents two separate unsafe actions: (1) operating the reactor at an inadequate level to prevent air entrainment to the DHP, and (2) providing inadequate preventive maintenance on the suction valve in the redundant loop. These two unsafe actions are separated well in time (though there is no explicit statement of when the valve was last maintained), and involve different departments within the plant. No common procedures, displays or other PSFs would seem to be implicated. Because one unsafe action was active, and one latent, no specific dependence mechanisms were discernible in this event. The prolonged operation at a reduced RCS water level was caused by operators not maintaining an adequate inventory, with deficiencies in related procedures and instrumentation.

The failures may be represented in a PRA as a failure of an operating pump to continue running resulting from an instrumentation problem with an independent failure of the redundant train (hardware failure). Recovery actions could have been dependent on the instrumentation fault, the cause of the pump failure, if the faulty "high level" indication had misled operators into starting another pump that also would have become air-bound.

C.A.1.2 Loss of Decay Heat Removal, Arkansas Nuclear One Unit 1, 10/26/88 (LER 313-88-014, Rev. 0)

In this event, an instrumentation and control (I&C) technician erroneously removed an unmarked fuse in a control-room panel, believing that it was to a strip-recorder he was about to remove. It actually supplied power to the controllers of two decay (residual) heat removal (DHR) cooler outlet valves, one in each redundant loop. Because of pre-existing wiring errors, the valves closed instead of opening on loss of control-signal supply. The event was recovered about 20 minutes later by operators checking on the work done by the I&C technician who restored the fuse.

The first unsafe action, of miswiring the valve controllers, had occurred significantly earlier than the second, the removal of the wrong fuse. This combination of unsafe actions is unlikely to be represented explicitly in any PRA. In practice, these would be combined into one event, an initiating event associated with complete loss of DHR (RHR) flow and added to other events in the same class to provide a frequency estimate. No separate analysis of possible dependencies between the unsafe actions would be necessary.

C.A.1.3 Loss of RCS Makeup, Arkansas Nuclear One Unit 2, 5/4/88 (LER 368-88-008, Rev. 1)

In this event, the normal and emergency makeup to the RCS was lost because the volume control tank (VCT) that supplies the chemical and volume control system (CVCS) was pumped dry. The VCT was emptied because of an erroneous "high level" signal generated by a VCT level transmitter incorrectly installed during the outage. The incorrect installation occurred because of deficiencies in the installation procedure and led to draining of the reference leg. The drained reference leg affected both redundant level channels.

Because of the erroneous high-level reading, the operators started the redundant charging pump but no flow resulted. Recovery occurred after the operators sent a local plant operator to check on the charging pumps who found no water when the vent valve was opened and no water came out.

Again, two unsafe actions occurred, with the second (emptying the VCT) caused by the first (incorrect installation of the level transmitter). These, it seems, should be modeled as a loss of makeup to the RCS (a single basic event) caused by instrumentation errors. Recovery would need to be modeled as conditional on the instrumentation problems, since it takes longer to detect the causes and leads the operators into taking actions that make the situation worse (like starting the standby pump that then becomes air-bound).

C.A.1.4 Excessive RCS Draindown, Waterford Unit 3, 7/14/86 (LER 382-86-015, Rev. 0)

Operations personnel were draining the reactor coolant system (RCS) to perform work on the reactor coolant pump (RCP) seals. The system was being drained using: (1) the low pressure safety injection (LPSI) pump mini-recirculation line to the refueling water storage pool (RWSP), and (2) the CVCS system to the holdup tanks. When intending to stop draindown, only the second path was isolated. The draindown continued until the LPSI pump ran dry and cavitated.

The failure to isolate all drain paths was compounded by inaccuracies in, and operator's suspicions about, the level indication. Problems with the local level indication were caused by the inability to supply nitrogen overpressure fast enough to compensate for the removal of RCS inventory, which led to the tygon tube undergoing a slight vacuum. (The installed level instrumentation of the reactor vessel monitoring system was also suspected as being wrong.)

Once the LPSI pump cavitated, the operators recognized that there was a drain path still open and closed it. The redundant LPSI pump was started and the RCS refilled from the RWSP without difficulty. RHR was eventually reestablished by repeated jogging of the original LPSI pump until cooling flow was restored after about 3 hours 45 minutes.

In terms of a PRA model, this event represents an "uncontrolled" overdraining of the RCS with an associated instrumentation failure. The failure of the instrumentation has the potential to make the recovery more complex by misleading the operators on the reason for the pump's failure, leading to use of parallel pumps that also become air-bound, and delaying refilling of the vessel.

C.A.1.5 Loss of Offsite Power, Shearon Harris, 10/11/87 (LER 400-87-059, Rev. 2)

This loss of offsite power occurred when construction staff jarred the protection relays for the one incoming supply line while the other was being modified.

Independently, testing the controls of the service water valves led to the failure to switch to the ESW supply on loss of offsite power. This is required to ensure cooling of the diesel generator, which started when offsite power was lost. The operators performing the testing recognized what had happened and restored the circuit from the testing. The valves were aligned manually as required.

The causes of the loss of offsite supply and the failure of the valves appear to be independent. Certainly, there is no basis for allocating any significant level of probability of their being related. Each failure would be binned into the appropriate frequency count for losses of offsite power and valves not changing when demanded.

C.A.1.6 Loss of RHR, Catawba Unit 1, 4/22/85 (LER 413-85-028, Rev. 0)

This event occurred when a draindown of the RCS was initiated with one loop of RHR unavailable for maintenance (a breach of technical specifications). The pump in the second loop became air-bound when operators over-reduced the RCS level. Over-reduction was caused by deficient level indication, which may have been caused by the hydrodynamic effects of a high rate of draindown in combination with an inadequate sensor range. RHR was recovered by stopping the draindown, adding inventory, and venting and restarting the RHR pump. RHR was restored within about 18 minutes from the initial termination of flow on air-binding.

The first unsafe action, initiating draindown with one loop of RHR unavailable, played a minimal role in the sequence of events. Its being available might have speeded up the recovery by avoiding the need for venting and refilling the failed pump. However, in terms of the sequence initiation from overdraining, the initial unsafe action does not appear to influence the occurrence of overdraining, either in terms of making it more likely or to change its consequences. Therefore, representation in the PRA would be as (1) unavailability of one loop of RHR on a relative-frequency basis, and (2) inadvertent overdraining, with this event being counted in the frequency of initiation of such events.

C.A.1.7 Loss of Offsite Power, Vogtle Unit 1, 3/20/90 (LER 424-90-006, Rev. 0)

During a refueling outage at Unit 1 of Vogtle NPP, a delivery truck struck a support for one of the phases of the in-service reserve auxiliary transformer feeding supplies to the shutdown unit. The duty Diesel Generator (DG) started but then tripped. Since the redundant supply paths and DG were out-of-service for maintenance, the tripping of the DG led to loss of RHR. The DG tripped several times because of deficient jacket-temperature sensors. These were overridden using the "emergency start" manual command, with RHR being restored after a break of 55 minutes.

The two failures (striking the electrical support and the faulty DG temperature switches) are considered independent. The cause of loss of electric supplies can be binned to be included in the frequency of such initiating events, and the failed switches represent on occurrence of a DG failing to start on demand.

C.A.2 REVIEW OF AIT AND AEOD HUMAN FACTORS REPORTS

C.A.2.1 LOCA with Loss of RHR, Braidwood Unit 1, 12/1/89 (AIT Report 50-456/89-03 & Table 6 of Ref. 5)

This event was initiated when a RHR pump suction relief valve spuriously opened in a non-operating RHR loop. It was caused by earlier inadequate maintenance (PSFs: human engineering and procedures). In response to this LOCA, the operators closed down the operating RHR loop (on the basis that "failures always occur in the operating loop"). Using the full-power LOCA diagnosis procedures in this shutdown event took a long time before operators eventually discarded them. Ultimately, training for this mode of operation helped operators solve the problem - after 131 minutes.

In this event, the same PSF (procedures) was implicated, though the instances of application were separated in time (pre-accident versus recovery) and occurred in separate plant groups (mechanical maintenance versus operations). In addition, the nature of the two deficiencies was somewhat parallel though not the same. In the case of the valve maintenance, the procedure was ambiguous about the steps for setting the setpoint; for the operators, the procedure was apparently not well prepared for non-full power operations. In these two cases, the deficiencies were due to an extensive lack of attention to all possible steps in a task. This is considered to be an instance where the process of generating and reviewing (formalizing) procedures represents a deficient common process.

From a PRA perspective, the spurious opening of the relief valve was an initiating event that was the result of an unsafe action (failing to maintain the valve correctly). In current PRAs, this would be assessed on the basis of historical experience, probably on a generic basis, and without specifically identifying the human contribution. Based on our findings, pre-accident human failure events should be identified explicitly to allow potential dependencies to be considered (see Section C.4). The delay in recovery would not necessarily be considered a human failure event in a PRA; this would be determined by assessing such factors as the time available for restoring core cooling before the onset of fuel damage. However, the quantification process, envisioned as a product of Task 10, would consider the factors in evidence here (like prolonged reliance on a marginally relevant procedure) in developing judgements about the probabilities of failure in other similar scenarios.

C.A.2.2 Loss of Essential Electrics, Diablo Canyon Unit 1, 3/7/91 (AIT Report 50-275/91003 and Table 7 of Ref. 5)

Two separate unsafe actions were involved in this event: a mobile crane touched the only incoming power line to Unit 1 in the switchyard and previously, some essential loads (control-room lighting, HVAC) had been switched to non-essential buses. At the time of this event, two new fuel assemblies were being transferred and were left initially motionless in the containment. The level of decay heat in the reactor was low. The emergency diesel generators started and loaded as designed, and all necessary reactor cooling systems operated. The fuel elements were moved manually.

While this event would be represented in a PRA as a loss-of-offsite-power initiating event, the possibility existed for other essential loads to be switched to non-essential supplies. If these other essential loads had been associated directly with core-cooling equipment or other similar safety equipment, the consequences could have been more significant. Also, the movement of fuel was interrupted because of the loss of electrical supplies. Other fuel-handling scenarios could presumably have been more significant in terms of personnel hazards. This event should be included in such other fuel-handling hazards.

The dependencies between the two unsafe actions existed in terms of common PSFs involving communications, and an organizational factor associated with coordinating and supervising work. The communications PSF was represented in the crane accident because the foreman considered (and should have) contacting operations to check whether the line was "live", but instead, made a wrong assumption. In addition, the transfer of the essential loads was not communicated to operators or other station staff. Similarly, with the organization factors, there was no administrative control over the movement of vehicles in the switchyard, and switching of the loads was uncoordinated with operations responsible for controlling the plant's configuration.

From a PRA perspective, no specific causes are identified for most losses of offsite power occurring at full power; rather, frequencies of loss and their duration are considered on a historical basis (i.e., what has been the history of such losses at the plant or within the region of the plant). Losses during low-power and shutdown conditions can be treated similarly--that is, based on historical experience for groups of similar plants. Low-power and shutdown operations have more frequent losses because of the increased amount of work performed on switchyards and related equipment during outages. Estimations of the frequency of such events should consider this increased frequency. The second event, the incorrect alignment of essential loads, is a failure rarely included in PRAs, However, this event has an increased potential during outages since the opportunities for errors of commission are increased (see the report for Task 7). In addition, such combinations of loss of offsite power and incorrect alignment of essential loads, as seen in this event, must be considered to be potentially dependent.

C.A.2.3 Loss of RHR, Oconee Unit 3, 3/8/91 (AIT Report 50-287/91-008, AEOD Human Factors Report, May 1991, and Tables 8 & 12 of Ref. 5)

This event is summarized in Table C.1 above from a human factors perspective; the following relates to the PRA perspective. It was set up by the inadvertent installation of a blind flange on the wrong sump suction line to the low pressure injection (LPI) pump of the RHR/LPI system. A subsequent inspection of the work failed to detect the error. The loss of residual heat removal (RHR) resulted from instrumentation and electrical (I&E) technicians performing a valve stroke test in the line that should have had the blind flange installed. Stroking the valve caused a drain path from the RCS to the containment sump, and as a result, suction to the running RHR/LPI pump was lost. A lack of coordination between operators and the technicians resulted in the operators not being aware that the valve-stroke test had started. Because of other concurrent plant activities and a history of unreliable instrumentation, the symptoms were not immediately interpreted. The area radiation monitors were out-of-service because of a plant modification in progress and the containment was only partly evacuated.

There are three phases to this event that are important in any PRA. First was the installation (and non-detection) of the blind flange in the wrong line. As described in the event report, many human-factors and organizational factors led to this failure. Second was the performance of the valve stroke test without coordination with the control room. While the test itself caused the drain path, coordination with the operators would have: (1) led them to stop the running LPI pump, thereby preventing its air-binding; and (2) prepared them to diagnose the cause of the event. As it was, RHR cooling was lost for 18 minutes because of the initial delay in diagnosis and the need to restore the pump's operation. The third was the deficiencies in evacuating the containment because of the inoperable area radiation monitors; this would be important in a modified level II PRA.

In terms of the influences, the uncorrected installation of the blind flange was predominantly a human-factors concern (inadequate plant labeling) though the procedures used were deficient in not being more

explicit about the location of the equipment. In addition, organizational factors (work practices, such as over-reliance on earlier work and a lack of checking before beginning a potentially significant operation) led to inadequate checking. The loss of LPI suction resulted from a lack of coordination between technicians and operators, partly because the procedures did not require this. The lack of operational area radiation monitors was an organizational deficiency since no alternate monitoring was required when the installed equipment was taken out of service. In summary, "procedures" was a common PSF for the flange installation error and the testing of the suction valve. "Organizational factors" was common to the flange installation error and the lack of area monitors. These common PSFs were separated in time and affected multiple organizational units; therefore, the potential for common processes underlying these common PSFs must be considered.

C.A.2.4 Loss of RCS Pressure, Crystal River Unit 3, 12/8/91 (AEOD Human Factors Report, January 1992 and Table 13 of Ref. 5)

While at 10% power during startup, inadequate maintenance of a pressurizer spray valve actuator (part missing) led to a stuck-open valve that was indicated closed. The primary system pressure fell but was interpreted by the operators as an overcooling event so they initially bypassed operation of the ESFAS. Subsequently, ESFAS was placed in operation and HPI restored RCS pressure above 1500 psig under manual control. After 1 hour, the spray block valve was closed, terminating the loss of pressure.

There were two unsafe actions: inadequate maintenance of the spray valve actuator, and a delay in controlling the loss of pressure. The PSFs associated with the inadequate maintenance were never reported. It would seem that no functional testing was performed following the maintenance, but why there was no testing is not known. The delay in diagnosing and responding to the loss of pressure is reported to have been driven by several PSFs, including poor procedures, human-machine interface, communications, and organizational factors. Any of these also could be a contributor to the failure of the spray-valve. Therefore, it is considered likely that there were common PSFs between the two unsafe actions, though the specific PSFs cannot be identified.

C.A.2.5 Loss of RHR, Prairie Island Unit 2, 2/20/92 (AIT Report 50-306/92-005, and Table 9 of Ref. 5)

The loss of RHR occurred when operators overdrained the RCS while going to midloop. While the causes of the overdraining were extensive and the responsibility was shared among different groups, the event was simple in the PRA context. It was an overdraining of RCS leading to loss of suction for the running RHR pump, with the consequence that recovery required venting and refilling of the RHR loop and RCS. No pre-accident failures (other than the design of the draining procedures and associated instrumentation) or errors during recovery occurred. Therefore, this event would be counted as a contributing event to the frequency of this class of PRA initiating event.

C.A.2.6 Inadvertent RCS and RHR Overpressurization, Catawba Unit 1, 3/20/90 (AEOD Human Factors Rpt., May 1990 & Table 10 of Ref. 5)

A scheduling error left three RCS pressure instruments out-of-service during repressurization of the RCS following a refueling outage. As a result, the operators overpressurized the RCS. In doing so, the RHR suction pressure relief valve opened and vented to the pressurizer relief tank (PRT), which was noticed by the operators. In diagnosing this PRT level, operators became aware of the high RCS pressure through indirect measurements, and increased the letdown flow to reduce RCS pressure.

From a PRA perspective, two connected failures occurred. First was the failure to ensure that the RCS pressure instruments (the primary operator interfaces) were in service, and second was the overpressurization that resulted from operators not monitoring the pressure. These are not directly dependent because the opportunity existed for the operators to monitor pressure from a variety of sources, but they failed to do so until the PRT level signal required diagnosis. The PSFs associated with the first failure were organizational factors and procedures, and with the second were training. Therefore, there were no common PSFs.

C.A.2.7 Loss of RCS Inventory, Braidwood Unit 1, 10/4/90 (AEOD Human Factors Rpt., October 1990 and Table 11 of Ref. 5)

This loss of RCS inventory resulted from two procedures being performed concurrently with no effective command and control. As a result, RCS was aligned to a valve to which the tygon tube (temporary level measurement) was connected. The tygon tube burst and sprayed personnel with hot (180^{0}F) RCS fluid. About 600 gallons of RCS inventory were lost. This event represents only one basic event in a PRA - a LOCA initiation.

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-6265
BNL-NUREG-52431

2. TITLE AND SUBTITLE
Multidisciplinary Framework for Human Reliability Analysis with an Application to Errors of Commission and Dependencies

3. DATE REPORT PUBLISHED
MONTH: August
YEAR: 1995

4. FIN OR GRANT NUMBER
L2415

5. AUTHOR(S)
M.T. Barriere,BNL, J. Wreathall, JW&Co., S.E. Cooper, SAIC, C.C. Bley, PLG, W.J. Luckas,BNL, A. Ramey-Smith, NRC

6. TYPE OF REPORT

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
Upton, NY 11973

Subcontractors
John Wreathall and Company, Dublin, OH 43017
Science Applications International Corp.,Reston,VA 22090
PLG, Incorporated, Newport Beach, CA 92660

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

10. SUPPLEMENTARY NOTES

11. ABSTRACT *(200 words or less)*

Since the early 1970s, human reliability analysis (HRA) has been considered to be an integral part of probabilistic risk assessments (PRAs). Nuclear power plant (NPP) events, from Three Mile Island through the mid-1980s, showed the importance of human performance to NPP risk. Recent events demonstrate that human performance continues to be a dominant source of risk. In light of these observations, the current limitations of existing HRA approaches become apparent when the role of humans is examined explicitly in the context of real NPP events. The development of new or improved HRA methodologies to more realistically represent human performance is recognized by the Nuclear Regulatory Commission (NRC) as a necessary means to increase the utility of PRAs. To accomplish this objective, an Improved HRA Project, sponsored by the NRC's Office of Nuclear Regulatory Research (RES), was initiated in late February, 1992, at Brookhaven National Laboratory (BNL) to develop an improved method for HRA that more realistically assesses the human contribution to plant risk and can be fully integrated with PRA. This report describes the research efforts including the development of a multidisciplinary HRA framework, the characterization and representation of errors of commission, and an approach for addressing human dependencies. The implications of the research and necessary requirements for further development also are discussed.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*
Probabilistic Estimation - Human Factors, Reactor Accidents - Human Factors, Reactor Operators - Risk Assessment, BNL, Errors, Failures, Functional Models, Human Factors Engineering, Nuclear Power Plants, Performance, Reactor Safety, Reliability, Working Conditions

13. AVAILABILITY STATEMENT
unlimited

14. SECURITY CLASSIFICATION
(This Page)
unclassified
(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE

Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

US NRC-OADM
DIV FOIA & PUBLICATIONS SVCS
TPS-PDR-NUREG
2WFN-6E7
WASHINGTON DC 20555

SPECIAL FOURTH-CLASS MAIL
POSTAGE AND FEES PAID
USNRC
PERMIT NO. G-67