An Analysis of Operational Experience During Low Power and Shutdown and a Plan for Addressing Human Reliability Assessment Issues

RECEIVED

AUG 0 8 1994

OSTI

Prepared by
M. Barriere, W. Luckas/BNL
D. Whitehead/SNL
A. Ramey-Smith/NRC

Brookhaven National Laboratory

Sandia National Laboratories

Prepared for
U.S. Nuclear Regulatory Commission

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

An Analysis of Operational Experience During Low Power and Shutdown and a Plan for Addressing Human Reliability Assessment Issues

Prepared by
M. Barriere, W. Luckas, Brookhaven National Laboratory
D. Whitehead, Sandia National Laboratories
A. Ramey-Smith, Nuclear Regulatory Commission

Contributors
D. Bley[1], M. Donovan[2], W. Brown[3], J. Forester[4], S. Cooper[5], P. Haas[6], J. Wreathall[7], G. Parry[2]

Brookhaven National Laboratory
Upton, NY 11973-5000

Sandia National Laboratories
Albuquerque, NM 87185

[1]PLG, Inc., Newport Beach, CA 92660
[2]HALLIBURTON NUS Environmental Corp., Gaithersburg, MD 20878
[3]Brookhaven National Laboratory, Upton, NY 11973
[4]Science Applications International Corp., Albuquerque, NM 87106
[5]Science Applications International Corp., Reston, VA 22090
[6]Concord Associates, Inc., Knoxville, TN 37932
[7]John Wreathall & Co., Dublin, OH 43017

ABSTRACT

Recent nuclear power plant events (e.g., Chernobyl, Diablo Canyon, and Vogtle) and U.S. Nuclear Regulatory Commission (NRC) reports (e.g., NUREG-1449) have led to concerns regarding human reliability during low power and shutdown (LP&S) conditions and limitations of human reliability analysis (HRA) methodologies in adequately representing the LP&S environment. As a result of these concerns, the NRC initiated two parallel research projects to assess the influence of LP&S conditions on human reliability through an analysis of operational experience at pressurized water reactors (PWRs) and boiling water reactors (BWRs). These research projects, performed by Brookhaven National Laboratory for PWRs, and Sandia National Laboratories for BWRs, identified unique aspects of human performance during LP&S conditions and provided a program plan for research and development necessary to improve existing HRA methodologies. This report documents the results of the analysis of LP&S operating experience and describes the improved HRA program plan.

Contents

Contents (continued)

Figure

Tables

Abbreviations

AEOD	NRC Office for Analysis and Evaluation of Operational Data
AIT	Augmented Inspection Team
AOP	Abnormal Operating Procedures
ASEP HRAP	Accident Sequence Evaluation Program Human Reliability Analysis Procedure
BWR	Boiling Water Reactor
CCW	Component Cooling Water
CDF	Core Damage Frequency
CR	Control Room
CVCS	Chemical Volume and Control System
CRO	Control Room Operators
DHR	Decay Heat Removal
EDG	Emergency Diesel Generator
EOC	Error of Commission
EOM	Error of Omission
EOP	Emergency Operating Procedure
EPRI	Electric Power Research Institute
ES	Engineered Safeguards
ESFAS	Engineered Safety Features Actuation System
ESW	Emergency Service Water
GGNS	Grand Gulf Nuclear Station
HACS	Human Action Classification Scheme
HPIP	Human Performance Investigation Process
HRA	Human Reliability Analysis (or Assessment)
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
IAE	Instrumentation and Electronics
IIT	Incident Investigation Team
INPO	Institute of Nuclear Power Operations
LER	Licensee Event Report
LOCA	Loss of Coolant Accident
LP&S	Low Power and Shutdown
LPI	Low Pressure Injection
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission (or U.S. NRC)
NUCLARR	Nuclear Computer Library for Assessing Reactor Reliability
NUMARC	Nuclear Utility Management and Resources Council
NSAC	Nuclear Safety Analysis Center
NSO	Nuclear Station Operator
POS	Plant Operational State
PRA	Probabilistic Risk Assessment
PWR	Pressured Water Reactor
PZR	Pressurker
RAT	Reserve Auxiliary Transformer
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RHRS	Residual Heat Removal System
RO	Reactor Operator
RV	Reactor Vessel

Abbreviations (continued)

SCRE	Shift Control Room Engineer
SCSS	Sequence Coding and Search Scheme (for LERs)
SDC	Shutdown Cooling
SE	Shift Engineer
SFP	Spent Fuel Pool
SLIM/MAUD	Success Likelihood Index Methodology/Multi-Attribute Utility Decomposition
THERP	Technique for Human Error Rate Prediction
TS	Technical Specifications

Definitions

Human Error/Unsafe Action

Human error describes an inappropriate human action(s), and/or lack of action(s), that lead the plant to a less safe state. The term "unsafe action" is used interchangeably with human error, but more appropriately, does not infer that a human is the cause of the problem.

Error Effect

Active: The consequences (effect) of the unsafe action is immediately revealed.

Latent: The consequences (effect) of the unsafe action remains dormant until triggered by some event.

Error Mechanism

Slip/Lapse: an unsafe action where what was performed was not what was intended.

Mistake: an unsafe action purposefully executed, as intended, where the intention is erroneous.

Circumvention: an unsafe action that is a deliberate but non-malicious violation of safety rules often done for, what is assumed, a "good" reason.

Error Mode

Omission: Failure to perform an action that leads the plant to a less safe state.

Commission: Performance of an action that leads the plant to a less safe state.

Human Action Classes

Pre-accident: An unsafe action which occurs prior to an abnormal event or accident and is discovered during the course of the event (i.e., latent).

Initiator: An unsafe action which starts an abnormal event or accident (i.e., active).

Post-accident: An unsafe action which occurs in the response to the abnormal event or accident and fails to mitigate the consequences of the event.

Recovery: An action taken in response to an abnormal event or accident which leads the plant to a safer condition.

Performance Shaping Factors (PSFs)

PSFs are those influencing factors which affect human performance and reliability (e.g., procedures, training, communication).

Executive Summary

This report meets two objectives. First, it documents the results of parallel analyses of operating experience at Boiling Water Reactors (BWRs) and Pressured Water Reactors (PWRs), which were performed for the U.S Nuclear Regulatory Commission (NRC) by Sandia National Laboratories (SNL) and Brookhaven National Laboratory (BNL), respectively. The analyses of operating experience identified unique aspects of human performance in a low power and shutdown (LP&S) environment. Second, it discusses resulting program plans for research and development required to improve existing human reliability analysis (HRA) methodologies. HRA is an integral part of probabilistic risk assessments (PRAs). Although various approaches and methods have been proposed since the first HRA was performed as part of the Reactor Safety Study (WASH-1400) almost two decades ago, the technology associated with HRA is still not fully developed. Limitations of existing HRA approaches become particularly important when the role of the human is examined in the context of nuclear power plants during LP&S conditions.

In 1980, the NRC designated shutdown decay heat removal to be an "Unresolved Safety Issue." While early studies of this issue began to reveal the importance of the human contribution to plant safety during LP&S, several recent events (e.g., the Chernobyl accident and the Vogtle loss of offsite power incident), which occurred at plants during shutdown operations, increased concerns regarding human reliability. These and related LP&S events have led to a growing awareness of the need for improvements in HRA methodology. Specifically, HRA methods must address the LP&S operating environment, which creates a set of circumstances that are unique in their contribution to human performance and reliability. In November 1991, the Senior Consulting Group (SCG) for the NRC's LP&S Level 1 PRA Projects agreed with a joint recommendation made by BNL and SNL to identify the detailed HRA needs for LP&S from actual event data and to develop appropriate methodological improvements to be implemented in LP&S PRAs. Subsequently, two parallel projects (BNL for PWRs and SNL for BWRs) to analyze operational

experience during LP&S were initiated by the NRC in February 1992.

A common analysis approach involving three major tasks was implemented by the BNL and SNL research teams. The first task involved the review of recent NRC and industry reports (i.e., SECY 91-283, NUREG-1449, NUMARC 91-06, NSAC-156 & -157) to identify factors and characteristics that are unique to the LP&S environment in their contribution to human performance and reliability. For the second task, an analysis of event reports was conducted to identify and characterize the more critical types of human errors that occur during LP&S and to identify their potential causes or influencing factors. Finally, for the third task, interviews were conducted with knowledgeable NRC, industry, and utility personnel to augment information developed during the first and second tasks.

The first and third tasks were similarly implemented by the BNL and SNL research teams. For the second task, alternative strategies for selection of event reports were taken. Relatively few challenging LP&S events have occurred at BWRs, and therefore very few in-depth inspection reports are available. Consequently, the SNL research team opted for breadth by reviewing licensee event report (LER) summaries, in an attempt to gather as much general BWR information as possible. LP&S-related LER summaries were selected from 10 U.S. BWRs to provide a representative sample of the different types of BWR systems and containments.

The greater number of significant LP&S events at PWRs, enabled the BNL research team to focus on documents providing considerable detail about particular events. Three principal sources of data were used: (1) NRC Augmented Inspection Team (AIT) or Incident Investigation Team (IIT) reports, describing significant LP&S events, (2) NRC AEOD reports describing significant human factors LP&S events, and (3) full-text LP&S LERs. The AIT, IIT, and AEOD reports provide detailed and independent evaluations, by NRC and its contractors, of the circumstances of significant events.

The broad review of BWR events provided better statistics on numbers of events of each class, while the PWR in-depth analysis approach provided more detail on specific events. The in-depth analysis also identified more event specific human influences and dependencies, which provided important guidance for the development of an improved HRA methodology.

To classify and characterize the types of human errors occurring during LP&S and identify critical performance influencing factors, a human action classification scheme (HACS) was developed. The associated HACS data fields incorporated a variety of information sources and existing instruments (including Draft NUREG-1449, NUREG/CR-3905, IEEE Std. 805-1984, NUREG/CR-4639, and NUREG/CR-5655).

Based on the results of the BNL and SNL assessment of influences on human reliability four key issues were identified that have implications for future research activities:

(1) Results from LP&S event analyses indicate that errors of commission (EOCs) are the dominant mode of human errors and are important in all temporal phases of a PRA (pre-accident, initiating event, and post-accident). Since traditional HRA methods have provided less than comprehensive treatment of EOCs and little guidance regarding their analysis in the PRA context, there is a need to develop a modeling approach for EOCs. Such an approach should help the HRA analyst to constrain the search to important EOCs for inclusion in the PRA models and estimate the probability or frequency of each identified EOC.

(2) Dependent human actions were found to impact the progression of LP&S events. Such dependencies included, for example, temporal phase-crossings (e.g., initiator/post-accident and pre-accident/post-accident dependencies) and separate erroneous actions by several groups caused by incorrect labeling of equipment. Existing HRA guidance for modeling dependent human actions is not yet mature and standardized in its application to

full-power PRAs, and provides little guidance for scenarios seen in LP&S events. Therefore, development is required for methods to guide the analyst in identifying, modeling, and quantifying the probabilities of important dependency mechanisms in the LP&S PRAs.

(3) Several performance-shaping factors (PSFs) were identified as important influences. These included procedures, training, human engineering, planning, organizational factors, and communication. Some of these PSFs (such as planning, organizational factors, and communication) are different from those typically regarded as important to human errors modeled in full power PRAs. In addition, the analyses showed that human performance during LP&S conditions is frequently influenced by the synergistic effects of multiple PSFs. Enhancements to HRA techniques are necessary to accommodate additional LP&S PSFs as well as the effects of multiple PSFs on human performance.

(4) Unlike full-power conditions, large numbers of multiple concurrent tasks are possible during LP&S conditions. This has implications for both the PRA modeling process and the HRA quantification process. Methods must be developed to (1) identify tasks that result in an undesired state when performed concurrently, (2) incorporate the undesired states into the PRA models, and (3) provide estimates of the probabilities of adverse effects of these interactions in the PRA model.

In response to human reliability issues and research and development (R&D) needs identified as a result of the BNL and SNL assessments, a program plan for accomplishing these necessary HRA/PRA improvements was developed. The program plan describes a series of tasks that will lead to quantification methods for EOCs and human dependencies, guidelines for implementation, and a demonstration of the methodology through trial application. Completion of the tasks should satisfy the overall goal of the research and development effort, which is the improvement of human performance modeling and its integration into PRAs.

1.0 Introduction

1.1 Background

Human reliability analysis (HRA) is an integral part of probabilistic risk assessments (PRAs). Although various approaches and methods have been proposed since the first HRA was performed as part of the Reactor Safety Study (WASH-1400) almost two decades ago, the technology associated with HRA is still not fully developed. The limitations of the existing HRA approaches become particularly apparent when the role of the human is examined in the context of nuclear power plants (NPPs) during low power and shutdown (LP&S) conditions.

Human performance plays a much larger role during LP&S than during full power operations. At many NPP units, automatic control and safety functions may be disabled, most control room annunciation titles indicate alarm status, few technical specifications apply, and configuration-specific emergency procedures are unavailable. During shutdown conditions, operators continually change the reactor coolant system configuration to accommodate maintenance, testing and other shutdown related activities. The increased levels of maintenance and testing also result in fewer available safety and support systems and associated equipment. Thus the demands on humans, both in terms of the frequency and directness of interactions with plant systems and in terms of the decision-making requirements in the context of an accident, may be substantially increased during LP&S.

In 1980, the NRC designated shutdown decay heat removal to be an "Unresolved Safety Issue." Since that time, a significant amount of work has been conducted to investigate safety issues in the LP&S environment. Early investigations included the NRC's study of alternate decay heat removal concepts for light water reactors (NUREG/CR-1556), the industry review and safety analysis of residual heat removal experience in PWRs (NSAC-52), and the NSAC's residual heat removal PRA of the Zion Nuclear Plant (NSAC-84). While the results of these and other studies began to reveal the

importance of the human contribution to plant safety during LP&S, several more recent events, which occurred at plants during shutdown operations, increased concerns regarding human reliability. These events include the 1986 incident at Chernobyl which was attributable to human error during low power testing exercises, and the loss of residual heat removal (RHR) systems during LP&S at Diablo Canyon in 1987 (NUREG-1269) and at Vogtle in 1990 (NUREG-1410) which were also attributable to human error. These and other LP&S related events prompted a number of studies by the NRC (summarized in NUREG-1449), which in turn have led to a growing awareness of the need for improvements in HRA methodology to support LP&S PRA. These improvements will enable the PRA to realistically represent the unique human performance characteristics and associated risk during LP&S.

In November 1991, the Senior Consulting Group (SCG) for the NRC's LP&S Level 1 PRA projects agreed with the joint recommendation made by Brookhaven National Laboratory (BNL) and Sandia National Laboratories (SNL) that the detailed HRA needs for LP&S be identified from actual LP&S event data and that appropriate methodological improvements be developed and implemented in the LP&S PRAs. Subsequently, two parallel projects (BNL's FIN L-2415 for PWRs and SNL's FIN L-2539 for BWRs) for the analysis of operational experience during LP&S were initiated during a February 1992 meeting with NRC.

1.2 Objectives

This report meets two objectives. First, it documents the results of parallel analyses of operating experience at BWRs and PWRs, which were performed for the NRC by Sandia National Laboratories (SNL) and Brookhaven National Laboratory (BNL), respectively. The parallel analyses identified the unique aspects of human performance in a low power and shutdown (LP&S) environment. Second, it discusses resulting program

plans for research and development required to improve existing human reliability analysis (HRA) methodologies.

1.3 Outline of the Report

To meet the objectives described above, this report makes use of previous draft letter reports and other documentation which are provided in Appendices A - E. Section 2 provides an assessment of influences on human reliability during LP&S. Section 3 discusses human reliability findings based on the assessments described in Section 2. Section 4 summarizes the program plan developed to identify the research and development processes necessary to improve HRA methodologies. The appendices A - E provide the detailed results of the initial phases of this research project.

Appendix A, discussed in Section 2, provides a listing of field headings and sub-category examples for the human action classification scheme (HACS) data base fields. HACS was developed in order to properly account for, document, and classify the various types of human actions and the critical factors that have actually occurred during significant LP&S plant-specific events.

Appendices B and C, discussed in Section 3, provide the complimentary analyses of operating experience in BWRs and PWRs during LP&S. Appendix B contains the BWR Letter Report from SNL (submitted on October 9, 1992) and Appendix C contains the PWR Letter Report from BNL (submitted on August 7, 1992).

Appendix D, discussed in Section 4, provides the program plan proposal that was developed on January 29,1993 to identify the research and development process necessary to improve HRA methodologies.

Appendix E, discussed in Section 2, provides the protocol utilized for conducting interviews with NRC, industry (EPRI and NUMARC) and utility personnel which were conducted to supplement the data extracted from LP&S reported events and associated studies.

2.0 An Assessment of Influences on Human Reliability

2.1 Description of Human Action Classification Scheme (HACS)

In order to classify and characterize the types of human errors occurring during LP&S and to identify critical performance shaping factors (PSFs), a human action classification scheme (HACS) was developed using a variety of information sources and existing instruments, including NUREG-1449, NUREG/CR-3905, IEEE Std. 805-1984, NUREG/CR-4639, and NUREG/CR-5655.

The development of HACS was influenced by: (1) the important issues identified in reports related to LP&S conditions; (2) experience in evaluating event data for human performance issues; (3) the intention to store the collected information in a computer database; and (4) the process of applying the scheme to the specific LP&S event data examined during both BWR and PWR operational data evaluations. A summary of the information utilized and corresponding HACS fields is provided below. Table 2.1 identifies the specific HACS database fields. The complete description of the HACS database fields is provided in Appendix A.

Event information. (Fields 1-3) Information uniquely identifying each event includes: the document number (including plant docket number), a brief event description, and the time of occurrence (i.e., date and time).

Plant state and conditions. (Fields 4-7,23) The plant type and vendor, the status of the plant (i.e., Plant Operational States (POSs)), noteworthy plant conditions (i.e., plant configuration, equipment out of service, etc.), and the status of other units at the time of the event are noted. In addition, the automatic response of equipment as it pertains to effective event mitigation is recorded.

Event severity. (Fields 24-27) The severity of the event is estimated by noting, when reported, the fission product barriers breached and other radiological effects. Also, an assessment is made with respect to the uniqueness of the event to LP&S conditions and the general level of risk significance.

Human action information. (Fields 8-22,28) Collection of a variety of human action information is accommodated by HACS. All human actions (latent, initiating event, and recovery) are identified and briefly described. For each human action, information typically pertinent to human reliability analyses can be documented within HACS, as applicable: personnel type (e.g., control room (licensed) operator); activities being performed (e.g., maintenance, testing, operations); location of action (i.e., in-control room or ex-control room); error mode (i.e., omission or commission); error type (i.e., slips, mistakes, or circumventions); active or latent errors, and influences (e.g., procedures, communication, human engineering) on human performance. HACS also accommodates documentation of long-term corrective actions indicated in the event data which are pertinent to the human actions identified. Other information accommodated includes the system(s) involved and the human action descriptor (e.g., start pump, isolate leak).

Event initiator (Field 29) An indication of whether or not the human action was the event initiator (i.e, yes or no). Based on the initial classification of LP&S events, it was recognized that encoding whether a particular human action was the event initiator, would be desirable. Consequently, this field was added to HACS.

The event information collected and encoded into the HACS database is intended to serve four major purposes. First, each event is uniquely identified by the plant involved, the date of occurrence, and the impact of the event upon the plant (e.g., loss of shutdown cooling, loss of offsite power). Second, the plant configuration and available equipment at

Table 2.1.
Human Action Classification Scheme (HACS) Database Fields

Field 1 - Event or Document Identification e.g., LER-dkt/yr-#, AIT-dkt/yr-#, NUREG-#	**Field 15 - Human Action Descriptor** NUCLARR Level 1,2,3 (NUREG/CR-4639)
Field 2 - Event Description Summary high level description of event	**Field 16 - Error Mode** omission or commission as coded in SCSS
Field 3 - Event Date and Time mm/dd/yy and hhmm	**Field 17 - Error Type** slip, mistake, or circumvention
Field 4 - Plant Type/Vendor BWR or PWR/vendor	**Field 18 - Active/Latent Effect** active, latent (prior/after startup)
Field 5 - Unit Status Plant Operational States (POSs)	**Field 19 - Error Influences** HPIP classification with additions
Field 6 - Noteworthy Plant Conditions unusual equipment and/or plant configurations	**Field 20 - Recovery Time** time from failure to recovery in minutes
Field 7 - Other Unit(s) Status status of other unit(s) at same site	**Field 21 - Recovery Locus** control room or outside control room
Field 8 - Human Action Number & **Description** # of human actions with brief description	**Field 22 - Recovery Origin** basis for decision/action: skill, rule, knowledge
Field 9 - Responsible Personnel Type personnel types (NUCLARR Level 1 and 2) with additional types for LP&S operation	**Field 23 - Related Automatic Equipment** **Response** text description
Field 10 - Event Activity (Ongoing) SCSS "Personnel System Codes" with additional types for LP&S operation	**Field 24 - Fission Products Barrier** **Breached/Threatened** fuel clad, RCS pressure boundary, containment, effluent treatment
Field 11 - Human Action Location control room or outside control room	**Field 25 - Other Effects** text description
Field 12 - System Identification IEEE Std 805 - 1984, Table 1	**Field 26 - Level of Significance** major, minor, detectable, questionable
Field 13 - Component Identification NUCLARR Level 2 (NUREG/CR-4639)	**Field 27 - Unique to Low Power or** **Shutdown** Yes/No
Field 14 - Displays/Instruments/Controls **Identification** NUCLARR Level 3 (NUREG/CR-4639)	**Field 28 - Corrective Action Taken** long term remedy
	Field 29 - Event Initiator Yes/No

the time of each event is identified as pertinent to the initiation of the event and mitigation options. Third, based upon actual or potential consequences, each event's severity is assessed. Finally, but most importantly, human performance information is gathered in order to identify human reliability influences (i.e., performance shaping factors) associated human actions (i.e., initiators, latent errors, or recovery actions), and error modes (i.e., commission/ omission).

2.2 Assessment Approach

A common assessment approach was implemented by the BNL and SNL research teams to accomplish the objective of identifying human influences during LP&S conditions for PWRs and BWRs. This approach involved three major tasks:

1) Recent NRC and industry reports (i.e., SECY 91-283, NUREG-1449, NUMARC 91-06, NSAC-156 & -157) related to LP&S operations were reviewed. The primary goal of the literature review was to identify factors and characteristics that are unique to the LP&S environment in their contribution to human performance and reliability.

2) An analysis of event reports was conducted to identify and characterize the more critical types of human errors that occur during LP&S and to identify their potential causes or influencing factors. HACS was used to facilitate the extraction of the relevant event-specific information.

3) An interview protocol was developed and interviews were conducted with knowledgeable personnel from NRC, industry (i.e., Electric Power Research Institute (EPRI) and the Nuclear Management and Resources Council (NUMARC)), and BWR and PWR utility personnel. The goal of the interviews was to obtain supporting information regarding situations, human activities, and performance influencing factors important to development

of a plan for addressing human reliability issues for LP&S operations.

Although implemented separately for BWRs and PWRs, the approach for tasks 1) and 3) above were identical. For task 2) alternative strategies for selection of event reports were taken by each research team.

The BWR research team at SNL opted for breadth by reviewing the licensee event report (LER) summaries, in an attempt to gather as much general BWR information as possible, enhancing the generic BWR applicability of any conclusions drawn from the data. As outlined in Table 2.2, a total of 555 human actions from ten different BWRs were identified from LER summaries and classified into HACS. It appears that very few challenging LP&S events have occurred at BWRs, and therefore very few in-depth inspection reports are available. The strategy for selecting BWR LP&S related LER summaries was to provide a representative sample of U.S. BWRs. The ten BWR plants selected represented the different types of BWRs and containments and their relative frequency.

Because of the greater number of significant LP&S events at PWRs, the BNL research team was able to focus on documents providing a detailed description about particular events. Three principal sources of data were used. These were: (1) NRC Augmented Inspection Team (AIT)/Incident Investigation Team (IIT) reports, describing significant LP&S events, (2) NRC AEOD reports describing significant human factors LP&S events, and (3) full-text LP&S Licensee Event Reports (LERs). As depicted in Table 2.2, the PWR human action data presently classified into HACS includes only plant-specific event information obtained from the analysis of licensee provided full-text LERs. A total of 66 human actions from events occurring at 24 different PWRs were identified from full-text LERs and classified into the HACS database. The AIT, IIT, and AEOD reports provide detailed and independent evaluations (by NRC and its contractors) of the circumstances of significant events. The results from analyzing the AIT and AEOD reports are currently being classified into HACS.

Table 2.2. Implementation of Events Reviewed from HACS

Information	BWRs	PWRs
Type Reports	LER Summaries	Full-Text LERs
Number of Human Actions	555	66[1]
Number of Plants	10	24

[1] Included 39 human errors and 27 recovery actions.

Since there are literally thousands of LP&S-related LERs for PWRs mentioning human performance issues, the strategy used to date for event data sampling has been to concentrate on events referenced in Draft NUREG-1449. In particular, those PWR LP&S events which have been included in the evaluation were those used as part of the NRC AEOD special report which reviews operating experience during shutdown and refueling and the NRC Accident Sequence Precursor methods, as noted in Draft NUREG-1449.

With respect to the objectives of this report, the BWR in-breadth review provided better statistics on unique aspects of human performance during LP&S. The PWR in-depth analysis approach provided more detail on specific LP&S events. The in-depth analysis also identified more event specific human influences and dependencies which provided important guidance for the development of an improved HRA methodology.

2.3 Analysis of Human Actions

The analysis of human actions resulting from the assessment approach previously described is discussed in the following sections with respect to an examination of LP&S operating experience reviews, an analysis of BWR and PWR plant-specific events, and interviews with NRC, industry and utility personnel.

2.3.1 Examination of LP&S Operating Experience Reviews

The sources of information utilized in the examination of LP&S operating experience reviews included SECY 91-283, Draft NUREG-1449, NUMARC 91-06, and NSAC-156 & -157. The results from examining each source are summarized in the subsections below. Appendices B and C provide a detailed discussion on each review source.

2.3.1.1 Evaluation of Shutdown and Low Power Risk Issues, SECY-91-283

SECY letter 91-283, issued on September 9, 1991, provides a status report on the staff's evaluation of safety risks that are unique to LP&S conditions and provides a revised action plan for completing the evaluation. The results of the ongoing staff activities discussed in the letter and in its enclosures have now been described in detail in Draft NUREG-1449 (discussed in Section 2.3.1.2). However, an enclosure of the letter provided an action plan for addressing key issues related to LP&S conditions and for addressing some additional topics which warranted further evaluation. These included:

- Outage Planning and Control
- Stress on Personnel
- Need for Improved Training
- Need for Improved Procedures
- Technical Specifications
- Instrumentation for Shutdown Conditions

2.3.1.2 Shutdown and Low Power Operation at U.S. Nuclear Power Plants, Draft NUREG-1449

The evaluation described in NUREG-1449 was initiated following the NRC staff's investigation of March 20, 1990 event at the Vogtle Nuclear Plant. The goal of the evaluation was to provide a broad assessment of risk during shutdown, refueling, and startup. The analysis of LP&S conditions identified a number of important technical issues relevant to the LP&S environment. Five issues which were determined to be especially important included:

- Outage planning and control
- Stress on personnel and programs
- Training and procedures
- Technical Specifications
- PWR safety during midloop operation

2.3.1.3 Guidelines for Industry Actions to Assess Shutdown Management, NUMARC 91-06

This industry document provides guidance to utilities in how to prepare for specific hazard states in planning for and controlling an outage. Specific hazard states addressed include loss of shutdown cooling, loss of inventory, loss of electrical supplies, and inadvertent reactivity addition.

NUMARC 91-06 identifies and provides guidance in several areas of interest related to outage planning and control. These include procedures, contingency planning, and training. In addition, the importance of organizational factors was discussed with respect to integrated management and providing defense in-depth.

2.3.1.4 Residual Heat Removal Experience Review and Safety Analyses, PWR and BWR, NSAC-156 & -157

NSAC-156 & -157 provide reviews and analyses of RHR system operating experience and performance during LP&S operations at PWR plants between 1982 and 1989 and at BWRs between 1984 through 1989. The primary data source for the NSAC evaluations was LERs, supplemented by INPO and AEOD reports, although the events listed do not identify the subject plant. Consequently, it was not possible to identify fully the information required for the HACS database.

The summary descriptions provided in NSAC-156 & -157 were studied to identify human activities, errors and contributions from human reliability influences. The results of these studies indicate that there are numerous human-system interactions which can lead to problems during LP&S conditions. It is apparent that administrative controls, training, procedures, task design, information display, and overall planning need to be specifically tailored for the unique aspects of the LP&S environment. Moreover, any assessment of risk under LP&S conditions will have to consider apparent inadequacies in the support of human actions. This will require a careful analysis of the relevant tasks and factors which influence human performance and reliability during shutdown.

Because of the incomplete information presented in the event summaries provided in these studies, it is difficult to draw clear conclusions about the patterns of errors and actions from their review. However, most human actions identified were errors of commission, resulting from mistakes induced by inadequate man-machine interface, poor procedures or inadequate instrumentation.

2.3.2 Analysis of Plant-Specific LP&S Events

The following subsections provide a brief summary of the plant-specific BWR and PWR event analysis descriptions which are detailed in Appendices B and C.

2.3.2.1 Analysis of BWR Events During LP&S

As indicated in the Section 2.2, a total of 555 human actions from BWR events were reviewed and coded into the HACS database from summary LERs available from the Sequence Coding and Search Scheme database (NUREG/CR-3905). Although no systematic training or procedures for using HACS were provided, coding strategy was discussed among

Influences

the team members at several points during the task to help attain some level of consistency. However, since no measure of inter-rater consistency was obtained, the results of the LER review should be considered preliminary. Additional research will be necessary before the numerical data can be taken as more than approximations.

Not all LERs reviewed for the ten plants were coded into the data base. Some selection of LERs for coding was done on the basis of coder judgement concerning relevance of the event for study. For example, an LER reporting a Technical Specification violation for failing to post a timely fire watch may not have been coded. The HACS data base contains only events for which complete coding was attempted. For most of the plants, at least the last 5 years of LERs were reviewed, with ten years of LERs reviewed for some plants.

Summary statistics characterizing some of the human errors and influences associated with the events analyzed are given below. A detailed discussion and presentation of the results from the analysis of summary LERs is provided in Appendix B. The percentages and frequencies reported below reflect the number of times (out of 555 human error events) that an identified human action was indicated as falling into a particular category. In some cases statistics are provided for loss of shutdown cooling and loss of electrical power events as well as for the overall set of events.

Approximately 60% of the loss of shutdown cooling and loss of electrical power events involved test, calibration, maintenance, repair, or installation errors. As a consequence of analyzing LP&S events, less than 20% of the events were found to be related to operations. Accordingly, the majority of the errors involved personnel other than control room operators.

Overall, errors of commission accounted for approximately 60% of the total, with approximately 30% errors of omission. However, of the 60 loss of shutdown cooling events, 49 (over 80%) involved errors of commission, with slips and mistakes occurring in approximately equal proportions. For

the loss of electrical power events, 24 of 35 events (65%) involved errors of commission. Most of the losses of electrical power occur due to slips as opposed to mistakes. While errors having active effects accounted for only half of the overall errors, they were much more prevalent in the loss of shutdown cooling (50 of 60 errors) and loss of electrical power (25 of 35 errors) events.

Procedures were identified as an error influencing factor in 45% of the loss of shutdown cooling and loss of electrical power events. Supervision and training were each cited in approximately 30% of these events, while human engineering and organizational factors each appeared in approximately 20% of the events.

The findings described above highlight some of the more interesting relationships among the different classifications and provide at least some initial insights into the nature of the human errors occurring during LP&S.

2.3.2.2 Analysis of PWR Events during LP&S

As indicated in Section 2.2, the actual PWR event-related human action data used in the LP&S analysis were derived from three principal sources. These were (1) NRC Augmented Inspection Team (AIT)/Incident Investigation Team (IIT) reports describing significant LP&S events, (2) NRC AEOD reports describing significant human factors LP&S events, and (3) full-text LP&S Licensee Event Reports (LERs). The full-text LERs examined were those associated with the plant-specific events cited in Draft NUREG-1449.

The sources differed with respect to the amount of relevant information they contained. Full-text LERs typically contain more complete descriptions of events, often considering precursors and recovery actions in greater detail than found in the abstracts included in summary LERs available from the Sequence Coding and Search System (NUREG/CR-3905) database. The preferred data sources were NRC event-based reports, such as AIT, IIT, and AEOD reports, because of their detailed and independent evaluations of the circumstances of

Table 2.3

Typical Amount of Detail from Various Sources Using Vogtle "Loss of Offsite Power" Event (3/20/90) as an Example

Data Available	DATA SOURCE		
	Summary LER	Full-Text LER	NUREG-1410 - IIT
Type and number of human errors and recovery actions	Initiator: 1	Initiator: 1 Latent: 1 Recovery: 1	Initiator: 1 Latent: 3 Recovery: 2
Type and number of human reliability influences	Organizational Factors: 1	Organizational Factors: 1 Procedures: 1 Training: 1	Organizational Factors: 1 Procedures: 4 Training: 3 Communications: 1 Human Engineering: 2 Design: 1
Plant configuration information	• Refueling • Train B RAT & DG out of service (OOS) for maintenance	• After Refueling • Train B RAT & DG OOS for maintenance	• After Refueling • Train B RAT & DG OOS for maintenance • 9 "above" actual Midloop • Charging pump B OOS for valve maintenance • All SG nozzle dams removed, but only SG #1 and 4 primary manways replaced • Pressurizer manway removed • Containment equipment hatch removed

RAT = Reserve Auxiliary Transformer.
DG = Diesel Generator.
OOS = Out of Service.

NUREG/CR-6093

significant events. Furthermore, influences on human performance are often treated explicitly in AIT, IIT, and AEOD investigations, making the reports especially useful for the purposes of this study. Table 2.3 illustrates the typical amount of information found in summary LERs, full-text LERs, and NRC event-based reports, using the March 1990 Vogtle Unit 1 event as an example. In addition the table shows that the NRC event-based reports provide a greater level of detail on pre-existing plant conditions; the number, type, and other characteristics of human actions; and influences on human actions. This finding influenced the data evaluation strategy of this effort to emphasize the evaluation of full-text LERs and NRC event-based reports.

Results from analyzing the NRC AIT, IIT, and AEOD reports are incorporated into the discussion provided in Section 3.0. A detailed discussion of the results obtained from analyzing all the event specific data sources (full-text LERs and NRC event specific reports) is provided in Appendix C. The following provides a brief discussion of the human errors and influences associated with the 32 full-text PWR LER events analyzed. This discussion is based on the tabulation of selected findings from the HACS database. The classification of the analysis results from NRC AIT, IIT, and AEOD event based reports into the HACS database is currently in progress.

Of the 32 events reviewed, 17 involved loss of shutdown cooling. In addition, 7 events comprised loss of some form of electric power but without loss of shutdown cooling. Within the 32 events, a total of 39 errors and 27 recovery actions were identified and analyzed. Of the 39 errors, 18 were latent and 21 were active. In addition 30 of the 39 errors actively initiated the event and 9 were latent errors that caused a mechanical malfunction which, in turn, triggered the event.

The personnel types most frequently involved in the human errors identified as contributing to these events were contractor/vendor personnel (15 out of 39 errors) and maintenance/instrumentation technicians (another 11 out of 39 errors).

In terms of error modes, errors of omission were reported in only 9 of the 39 errors; the remaining 30 were errors of commission. The most frequently occurring errors of commission were the commission of undesired tasks, analyses or steps (17 out of 39 errors), with the next most frequent being errors of commission from other human factors, such as a faulty RCS level display (another 11 out of 39).

The error types most frequently identified overall were mistakes (26 out of 39 errors) of which 14 resulted from faulty or inadequate procedures with 8 more resulting from faulty diagnosis. Of the 13 slips identified, 10 were attributed to inadvertent actuation.

Recovery by human intervention (recovery actions) in most cases involved actions from both outside and inside the control room (17 out of 27). Only 7 events were recovered by human actions taken inside the control room alone; only 3 were recovered exclusively from outside the control room.

2.3.3 Interviews with Knowledgeable Personnel

2.3.3.1 NRC and Industry Personnel

Interviewees from NRC and Industry (EPRI and NUMARC) identified a number of challenges to plant safety associated with LP&S. Plant configuration when an event occurs was reported to have a significant impact on event severity and mitigation. Movement of radioactive fuel was also reported to impact safety. Examples of fuel being shuffled into locations which had been unanalyzed, and into loadings where instrumentation did not provide meaningful indications of approaching criticality, were cited. Other plant configuration characteristics reported to impact safety included the inability to close containment, reduced RCS inventory control, decay heat removal, and less than adequate control over switchyard activities.

It was reported that during LP&S, plant configurations change continuously and human-system interactions are much more frequent. There are

major configuration changes, more people, and an increase in diverse activities, thus making control and communication a more demanding task. The overall consensus was that LP&S was a more complicated and dynamic condition requiring a different approach than that of normal operation. Consequently, there is a much greater emphasis on the importance of communication, organizational factors, supervision, and stress associated with LP&S conditions.

Procedures and training were rated high in importance and applicable to both initiators and recovery of LP&S as well as full power events. A synergistic relationship was reported to exist between procedures and training such that if both were bad, the operators could really get into trouble. However, some interviewees reported that good training could compensate for inadequate procedures. Stress, communication, human engineering, supervision, and organizational factors were reported to be situation-specific with respect to their importance as potential contributors to human performance during LP&S. Training was reported to be of significant importance for maintaining plant safety during LP&S. It was stressed that with adequate training operators would not be surprised or ill prepared when unexpected or unanalyzed phenomena occur.

Poor outage planning was cited as being a significant contributor to many LP&S events. It was recommended that outage planning should focus on safety functions and not solely on desired equipment maintenance, and that vulnerabilities and contingency plans should be explicitly identified.

2.3.3.2 Interviews with BWR Utility Personnel

BWR plant personnel raised many of the same issues identified in the previous section (unfamiliar tasks, lack of relevant training, less well-defined procedures, fatigue, schedule pressure, workload stress, greatly increased demands on communication and coordination were all mentioned by interviewees). The influx of contract personnel not thoroughly familiar with the plant and not fully integrated into the shift operation is a recognized

issue. Tagging control was also identified a number of times as a significant issue that is very important during an outage due to the greatly increased activities and the changing, non-routine configurations.

Among the challenges to safety functions identified by interviewees were the transition to RHR during LP&S, a stop/hold during shutdown or cooldown, any major system evolution or alignment, and any evolution involving moving water from/to reactor cavity for refueling.

According to interviewees, good outage management was characterized by clear identification of critical systems on a day-to-day basis throughout the outage, complete and constant awareness of the state of the plant and equipment, good communication to all personnel, and tight control over the work in progress.

2.3.3.3 Interviews with PWR Utility Personnel

According to PWR personnel, the greatest challenge to critical safety functions comes from the possibility of simultaneous unavailability of equipment causing the loss of a given function. There was general agreement that operating with reduced RCS inventory under circumstances in which the RHR function might be compromised represented a serious challenge to the safety of the unit.

During an outage, the role of the operations staff changes considerably when compared with full power operation. The operating circumstances during an outage are more demanding, the work more intensive, and shift turnovers more difficult. Reduced inventory operations were identified as presenting the greatest challenge to the operator. Also noted as difficult were maintaining awareness of plant status, keeping track of unavailable equipment, and avoiding loss of information during shift turnovers. The number and complexity of the maintenance activities performed during LP&S operations is greatly increased. The tasks are also typically longer in duration than during full power

Influences

operations, so that communication during shift turnovers becomes an important factor.

Interviewees were in agreement that outage planning was important to the success of the outage. Maintenance personnel judged the availability of manpower and replacement parts to be critical to safe and timely completion of outage maintenance. Coordination and communication with operations personnel were also seen as important. Outage planning personnel emphasized that the success of an outage depends on close, continuing coordination with operations personnel and meticulous management of the plan as it evolves through multiple revisions.

3.0 Human Reliability Findings

Of all the various data sources discussed above, the results of analyzing NRC event-based data (AIT, IIT and AEOD reports) provided the most detailed information for identifying the LP&S human reliability findings discussed below. The examination of recent NRC and Industry reports (e.g., Draft NUREG-1449) provided useful back-ground information. Interviews provided general and plant-specific supplemental information on the data extracted from the reported events and associated studies.

The conclusions drawn from this research effort are that human actions and errors are significant contributors to risk during LP&S operations. In particular, the principal errors that seem important under such conditions are associated with manual control actions (e.g., reducing level) and control of equipment configuration for maintenance and test that lead to the loss of defense-in-depth. The quality of procedures and information systems (e.g., temporary instrumentation, annunciator tiles indicating alarm states, etc.), and control and coordination of plant status (e.g., inadvertently working on two trains) influence human performance and play an important role in the frequencies of errors in LP&S operations. Recovery actions are available for most kinds of problems, though failures during the early stages of an outage when decay heat levels are still significant present greater challenges because of reduced time to core uncovery.

The findings of the assessment of influences on human reliability during LP&S can be organized into three areas for more detailed exposition: (1) a characterization of the human actions and errors that could have a significant impact on safety during LP&S operations; (2) an evaluation of primary influences on human performance during LP&S operations; and (3) a review of how these actions, errors, and influences differ from those human actions, errors, and influences important to safety during at-power operations.

3.1 Characterization of Human Actions and Errors

There is a consistency in results between the evaluation of data sources and the opinions of knowledgeable individuals interviewed for the project. For example, operations during outages identified as important to safety in both the event analyses and the interviews included lowering RCS water level and maintaining electrical supplies. During these operations, configurations can be encountered that make the plant more vulnerable to errors by personnel or failures of equipment. Examples include the limited margins for error in level control during PWR mid-loop operations, where vortexing may lead to loss of all RHR pumping. In particular, it is the unique combination of unusual plant vulnerabilities together with the increased opportunities for errors during unusual evolutions that make LP&S operations of concern.

Because human-system interactions during LP&S operations are more direct, with operators more frequently manipulating equipment and changing plant configurations, there is a greater opportunity for these interventions to go astray, resulting in mistakes leading to errors of commission. In many cases, these mistakes are the result of poorly developed procedures that fail to provide guidance in some part of an evolution, such as when the equipment does not operate as assumed in the procedure, or there is simultaneous work proceeding in another part of the system. This is reflected in the interview comments about the importance of outage planning and the need for LP&S-specific technical specifications.

Both latent and active errors appear to play a significant role. In most of the detailed event descriptions (i.e., AIT and AEOD report analyses), both latent and active failures were present to cause the situation. This was reinforced in the LER-based information where approximately 54 percent of the errors detailed were active and 39 percent were latent. In all three event-based reports (AIT, IIT,

and AEOD), active human error was found to be the most likely event initiator.

Recovery of failed safety functions was accomplished in all cases before plant damage occurred, usually through manual actions. A wide range of times until recovery was reported in both of the BWR and PWR operational event reviews. The longest times (> 4 hours) were often associated with situations where partial recovery of equipment occurred (as with venting of an RHR pump) only for the equipment to fail again (as when the cause of the pump air-binding was not corrected) before being finally restored. The shortest times (< 1 minute) involved simple switching actions in the control room such as reclosing a circuit breaker.

3.2 Evaluation of Primary Human Reliability Influences

As with the kinds of errors and actions, there seems to be a convergence in the findings of important human reliability influences from the evaluation of reports, events, and from the interviews. Through all the sources of information, the most frequently identified influence is procedures. That is, procedures and practices a plant uses to define and implement safety criteria for LP&S operation. These would include formal administrative procedures (e.g., Conduct of Operations - outage), shift orders, outage planning guidelines, Emergency Procedures, or informal practices observed by a significant portion of the staff.

The event data indicate that procedures are frequently deficient, either by providing inadequate guidance or in omitting instructions for unexpected contingencies while performing evolutions. This is especially troublesome with temporary procedures for special evolutions during shutdown. The interviews indicate procedures and training are rated highly as a human reliability influence, particularly in certain plant configurations when other influences come into play. These other situation-specific influences include human engineering, communications, organizational factors, and stress. This observation is again reflected in the interviews

and event data. The analysis of the more detailed AIT, IIT, and AEOD event-based reports identified multiple influences (e.g., procedures, human engineering, organizational factors, and communication) for specific events, achieving an effect of which each individual influence is incapable of. In addition, the generic data analysis also identified the importance of multiple influences, but in a broader sense. The synergistic effects of multiple influences are not practically considered in any commonly used human reliability methods and are therefore seen as an important finding in this research.

One observation from the interviews was that the safety concerns and influences are very situation-specific. This was not directly observable from the event data but could be inferred from the number of reports associated with specific plant conditions, most noticeably lowering PWR water level in the transition to mid-loop operations. Another situation-specific concern was the period where limited electrical supplies (on-site or off-site) were available. Electrical-related components and activities were associated with a large number of errors with potentially significant consequences. Typically, single errors were sufficient to initiate significant safety challenges in those conditions. In addition, in the case of changing to mid-loop operations in PWRs, the plant is in a dynamic state such that operators are more challenged in tracking parameters using (often inadequate) instrumentation and procedures.

Recovery actions were frequently aided by use of abnormal or other contingency procedures once an event had been initiated and (often) a safety function was lost. In addition, the detailed event analyses and the interviews indicated that training and the detailed technical knowledge of plant operators can be important in assisting in the recovery of lost safety functions and stabilization of the plant. However, the level of operator training in LP&S operations varies considerably and is expected to be a critical factor in the reliability of operator actions during off-normal events. Both classroom training on LP&S conditions, as well as simulator training, were identified as important factors. Furthermore,

for loss of shutdown cooling events in BWRs, supervision was identified as an influencing factor 40% of the time. This result implies that supervision, which can be thought of as an organizational practice, is an important factor affecting human actions.

In summary, the principal findings in terms of influences on human performance are that:

- Most events of any significance to safety involve multiple influences.

- The most frequently cited human reliability influences are procedures and human engineering.

- The more detailed descriptions of events indicate that these deficiencies are symptomatic of poor planning and preparation, as indicated by frequently concurrent deficiencies in training, communications, and organizational factors.

- The combinations of influences giving rise to performance problems appear to be very sensitive to the context of the plant conditions.

- Recovery is frequently aided by situation appropriate procedures, specific training, and the technical knowledge of the operations personnel.

3.3 Differences Between Full-Power and LP&S Operations

A number of significant differences between the human actions, errors, and influences important to LP&S operations and those important to full-power operations have been identified. Aspects of the following identified features are unique and important to LP&S operations: the kinds of human interactions and events; the classes, modes, and types of human errors (and actions); influences on human performance; and plant conditions and configurations.

Unlike full power operations, all classes of human actions and errors (i.e., initiator, pre-accident, and recovery) seem to play a significant role in LP&S operations and events. In particular, human-initiated events usually are not explicitly treated in full power PRAs. It is typically assumed that human-initiated events while at power can be captured in data collected at the component, system, or plant level and have no detrimental impact on response following the initiator. For LP&S events, however, human-induced initiators, both inside and outside the control room, comprise a significant portion of observed errors. In addition, there are frequently dependencies between the activities leading to the initiating event and those required for most expeditious recovery response.

The data evaluations indicated that mistakes (versus slips) and errors of commission (versus omission) predominate the types and modes of human errors which occur during LP&S. In addition, mistakes and errors of commission occur both inside and outside the control room during LP&S. The more direct human-system interactions characteristic of LP&S operations can result in mistakes which, in turn, lead to errors of commission. In contrast, the human errors explicitly modeled in full-power PRAs are typically errors of omission (for example, the NRC Generic Letter 88-20 does not require errors of commission to be modeled in licensee Individual Plant Examinations), and when mistakes are included, only in-control room errors are typically modeled.

The data collection efforts of this endeavor have resulted in the identification of several important influences on human performance during LP&S. The evaluation of reports, event-based data sources, and interviews identified procedures, human engineering, training, organizational factors, and communications as significant contributors to human errors and actions.

Procedures are important in modeling human errors in full-power PRAs. However, human engineering (especially in the control room), organizational factors, communications, etc. are not typically incorporated as influences on human performance at

full power. In addition, the event-based data evaluations strongly indicated that contributions from multiple influences are common for human actions and errors during LP&S. Also, the available time for event response, frequently an important factor in human performance at full power, does not appear to be as critical during LP&S. (Exceptions are likely for events initiated shortly after shutdown when decay heat is high and for events that can progress unnoticed for extended periods of time).

In the context of nuclear power plant operations, workload and stress are often closely related. Increased workload and stress were often cited in the literature as contributors to human error during LP&S. The presence of a much larger staff including less experienced personnel, at the plant, as well as the influence of extended work periods, can play significant roles in increasing the workload of operators. However, the plant staff interviews indicated that high workload and stress, while potentially significant during LP&S, did not appear to be at detrimental levels at the plant. It was stated that during an outage, the size of the operations crew is expanded and the shift organization is changed to minimize the impact of the increased workload and to reduce the stress of outage operations. These measures were cited by the staff as effective in minimizing the impact of outage operations on workload and stress. Perhaps staffing and organizational factors can be used as influencing factors rather than the more difficult to measure factors of workload and stress.

Unlike full power operations, LP&S operations are performed under complicating conditions. For example, much greater emphasis is placed on manual control actions. Also, personnel not normally at the plant (e.g., headquarters engineers and contractors) and others not intimately familiar with the plant's day-to-day work practices and normal operating procedures may be performing tasks that can affect safety. In addition, problems can exist in terms of the operators' ability to observe the state of the plant and the configuration of its equipment. Finally, operators face continuously changing plant conditions and configurations. Frequent changes in the plant situation result in changes in the potential consequences of events and the availability of redundant (and, in some cases, front-line) equipment in event responses. In addition, the changing plant environment during LP&S increases the importance of communications in order to safely perform outage activities and to appropriately respond to LP&S events. Also, equipment is more frequently manually operated during LP&S operations, and responses to LP&S events are typically achieved through manual human actions rather than automatic equipment response.

These differences from full power operations help create a situation where errors are more likely and their consequences less observable. However, a significant mitigating factor is that, after the first few days of an outage, the time required for fuel uncovery to occur following loss of cooling, for example, is sufficiently extended so that delays in recovering from errors can be tolerated with less impact on risk.

4.0 Implications for Research

After having completed the assessment of influences on human reliability for BWRs and PWRs, various implications for the HRA/PRA process became apparent. In the following sections, these implications and a plan for addressing them are discussed.

4.1 Assessment of Human Reliability Issues

Four key human reliability issues are identified as a result of the assessment of LP&S events that have implications for future research and development activities. Each is discussed below.

Analysts must incorporate EOCs into LP&S PRA modeling.

To adequately represent LP&S conditions in a PRA, analysts must be able to incorporate errors of commission (EOCs) into the PRA models. Results from LP&S event analyses indicate that EOCs are the dominant mode of human errors and are important in all temporal phases of a PRA (pre-accident, initiating event, and post-accident). Unfortunately, traditional HRA methods have provided less than comprehensive treatment of EOCs and little guidance regarding their analysis in the PRA context. Consequently, there exists a need to develop a modeling approach which more adequately addresses EOCs. Such an approach should help the HRA analyst constrain the search for EOCs to those of most relevance to the PRA models and estimate the probability or frequency of each identified EOC.

Dependencies between human actions are frequent.

The assessment of LP&S events also revealed that dependencies between human actions occur relatively frequently. These dependent human actions impact the progression of LP&S events. Such dependencies include, for example, temporal phase-crossings (e.g., initiator/post-accident and

preaccident/post-accident dependencies) and separate erroneous actions by several groups caused by incorrect labeling of equipment. Existing HRA guidance for modeling depedent human actions is not yet mature and standardized in its application to full-power PRAs, and provides little guidance for scenarios seen in LP&S events. Therefore development is required for methods to guide the analyst in how to identify, model, and quantify the probabilities of important dependence mechanisms in the LP&S PRAs.

Additional PSFs (and their associated synergistic effects) are important.

Several performance-shaping factors (PSFs) were identified as important influences in the data analyses. These include procedures, training, human engineering, planning, organizational factors, and communication. Some of these PSFs (such as planning, organizational factors, and communication) are different from those typically regarded as important to human errors modeled in full power PRAs. In addition, the analyses showed that human performance during LP&S conditions is frequently influenced by the synergistic effects of multiple PSFs. While existing HRA techniques provide mechanisms for incorporating the effects of PSFs into the quantification process, enhancements will be necessary to accommodate the additional PSFs as well as the effects of multiple PSFs on human performance.

Multiple, concurrent tasks are often performed.

Unlike full power conditions, large numbers of multiple concurrent tasks are possible during LP&S conditions. Examples of important multiple concurrent tasks include simultaneous performance of different surveillance tests which create multiple RCS draindown paths and/or maintenance activities which result in identical plant conditions (e.g., increasing sump or tank volumes) to those caused by control room errors, thereby hindering diagnosis of LP&S events. This has implications for both

the PRA modeling process and the HRA quantification process. It would be useful to develop methods to: (1) identify the tasks that, if performed concurrently, would result in an undesired state; (2) provide a means of incorporating this undesired state into the PRA models; and (3) provide estimates of the probabilities of adverse effects of these interactions in the PRA model itself.

In addition to the four key issues identified above, several additional issues were identified as having implications for future research. Errors important to safety, particularly those that initiate events, are very context-specific. Consequently, the context in which actions are taken should be accounted for and may require more information about dynamic plant conditions than a typical PRA cutset scenario provides. Also commonly used techniques for modeling recovery actions do not take into account the possible complexities of restoring mechanically failed or disassembled equipment.

It is acknowledged that this assessment of LP&S events has precluded the identification of high consequence, but low probability human errors that have not yet occurred, and therefore have not been encoded into HACS. These types of insights and a means for addressing them will be included as part of the quantification task (subtask 4.3) discussed in the following section.

4.2 Development of Plan For Addressing Human Reliability Issues

In response to the human reliability issues and research and development (R&D) needs described above, a development task (program) plan for accomplishing necessary HRA improvements was developed. A flow diagram of the resulting integrated HRA/PRA program task plan is presented in Figure 4.1 and discussed below. The complete program plan outline is provided in Appendix D.

This report comprises the product of Task 1 of the program plan. Of the remaining tasks shown in Figure 4.1, four tasks will be pursued in the near

term. Tasks 2 and 3, and Subtasks 4.1 and 4.2 are planned for the next phase of this project. Subtask 4.3, and Tasks 5 and 6 are anticipated to be performed in the next fiscal year. Subtask 4.4 has been postponed to a later time due to present resource constraints.

The overall goal of the R&D effort, represented by these tasks, is to improve human performance modeling and its integration into the PRA. The specific objectives of each technical development task are summarized below.

- Task 2: The identification of user requirements through interviews with prototypical end-users about the kinds and levels of guidance required, and constraints imposed by technological aids.

- Task 3: The refinement of an HRA framework, which will serve as a unifying "skeleton" for the subsequent development tasks. The explicit use of such a framework is unique in the development of HRA methods. This framework will provide a logical and explicit basis for incorporating human failure events into PRAs that is consistent with the knowledge about the consequences and rates of occurrences of different types of human errors. It should also describe the relationships between human errors as considered in the behavioral sciences (e.g., Reason, 1990) and the human failure events as considered in the PRA systems-analysis tasks.

- Subtask 4.1: The development of a method for identifying and representing Errors of Commission. The method should provide a mechanism for limiting the search through the essentially unbounded number of possible inappropriate actions.

- Subtask 4.2: The development of a method for dealing with the dependencies among human errors. This method should account for the various performance influencing factors identified during the assessment discussed earlier.

- Subtask 4.3: Enhancements to, or development of, a quantification process. This process should

provide the HRA/PRA analyst with a means to appropriately quantify the human actions incorporated into a PRA.

- Subtask 4.4: The development of an approach for incorporating multiple, concurrent tasks into PRAs. This approach should provide the analyst with the means of representing the dynamic nature of the plant during LP&S conditions. This task will be postponed, as noted above.

- Task 5: The development of guidelines on how to use the newly developed HRA/PRA methods. These guidelines are to be written such that the intended users can apply the developed HRA/PRA methodology.

- Task 6: Demonstration of the applicability of guidelines through a trial application on an appropriate PRA and refinement of the guidelines based on feedback from the trial applications process.

Figure 4.1 Integrated HRA/PRA Program Plan Tasks - Flow Diagram

5.0 References

AEOD Human Factors Team Report - Catawba, Unit 1 - March 20, 1990, "On-Site Analysis of the Human Factors of an Event," U.S. Nuclear Regulatory Commission, May 1990.

AEOD Human Factors Team Report - Braidwood, Unit 1 - October 4, 1990, "On-Site Investigation and Analysis of the Human Factors of an Event," U.S. Nuclear Regulatory Commission, October 1990.

AEOD Human Performance Study Report - Oconee, Unit 3 - March 8, 1991, "On-Site Analysis of the Human Factors of an Event (Loss of Shutdown Cooling)," U.S. Nuclear Regulatory Commission, May 1991.

AEOD Human Performance Study Report - 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, January 1992.

AEOD Human Performance Study Report - Prairie Island, Unit 2 - February 20, 1992, "On-Site Analysis of the Human Factors of an Event (Loss of Shutdown Cooling)," U.S. Nuclear Regulatory Commission, March 1992.

AEOD Special Evaluation Report, "Review of Operating Events Occurring During Hot and Cold Shutdown and Refueling," U.S. Nuclear Regulatory Commission, December 4, 1990.

Generic Letter No. 88-20, "Individual Plant Examination," U.S. Nuclear Regulatory Commission, November 1988.

IEEE Std. 805-1984, "IEEE Recommended Practice for System Identification in Nuclear Power Plants and Related Facilities, Table 1," Institute of Electrical and Electronic Engineers, 1984.

Inspection Report No. 50-306/92-005, Prairie Island, Unit 2, "Loss of RHR (February 20, 1992)," Augmented Inspection Team Report, U.S. Nuclear Regulatory Commission, March 17, 1992.

Inspection Report No. 50-275/91-009, Diablo Canyon, Unit 1, "Loss of Off-Site Power (March 7, 1991)," Augmented Inspection Team Report, U.S. Nuclear Regulatory Commission, April 17, 1991.

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

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

NSAC-52, "Residual Heat Removal Experience and Safety Analysis, PWRs," Electric Power Research Institute, January 1983.

NSAC-84, "Zion Nuclear Power Plant Residual Heat Removal PRA," Electric Power Research Institute, January 1985.

NSAC-156, "Residual Heat Removal Experience Review and Safety Analysis, PWRs, 1982-1989," Electric Power Research Institute, August 1991.

NSAC-157, "Residual Heat Removal Experience Review and Safety Analysis, Boiling Water Reactors, 1984-1989," June 1991.

NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management," NUMARC, December 1991.

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

References

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, June 1990.

NUREG-1449, "Shutdown and Low-Power
Operation at Commercial Nuclear Power Plants in
the United States," Draft Report for Comment, U.S.
Nuclear Regulatory Commission, February 1992.

NUREG/CR-1556, "Study of Alternate Decay Heat
Removal Concepts for Light Water Reactors:
Current Systems and Proposed Options," U.S.
Nuclear Regulatory Commission, April 1981.

NUREG/CR-3905, "Sequence Coding and Search
System for Licensee Event Reports," U.S. Nuclear
Regulatory Commission, April 1985.

NUREG/CR-4639, "Nuclear Computerized Library
for Assessing Reactor Reliability (NUCLARR),
User's Guide Volume 4," U.S. Nuclear Regulatory
Commission, October 1990.

NUREG/CR-5655, "Human Performance
Investigation Process (HPIP)," U.S. Nuclear
Regulatory Commission, 1991.

Reason, James T., Human Error, Cambridge
University Press, 1990.

SECY-91-283, "Evaluation of Shutdown and Low
Power Risk Issues," September 9, 1991.

U.S. Nuclear Regulatory Commission, Reactor
Safety Study, WASH-1400, October 1975.

APPENDIX A
HUMAN ACTION CLASSIFICATION SCHEME
(HACS)
DATABASE FIELD CATEGORIES

APPENDIX A
HUMAN ACTION CLASSIFICATION SCHEME
(HACS) DATABASE FIELD CATEGORIES -

Field 1 - Event or Document Identification
e.g., LER-dkt/yr-nnn, AIT-dkt/yr-nnn, NUREG-nnnn, or other as appropriate

Field 2 - Event Description Summary

1. Loss of Shutdown Cooling*
2. Loss of Reactor Coolant Inventory*
3. Breach of Containment Integrity* e.g., Inadvertent Actuation of Isolation Valves, Breach of Equipment or Personnel Air Locks.
4. Loss of Electrical Power* e.g., Failure of Emergency Diesels, Loss of Electrical Bus, Loss of Offsite Power.
5. Overpressurization of Reactor Coolant System* e.g., Solid RCS Pressure Control, Inadvertent Safety Injection.
6. Flooding and Spills* e.g., Radwaste Spills, Breach of Flood Dikes.
7. Inadvertent Reactivity Additions* e.g., Boron Dilution, Incorrect Control Rod Calibration.
8. Challenge To Fire Protection
9. Loss of Heat Sink e.g., Service Water, Ultimate Heat Sink
10. Quality Assurance Inspections & Infractions. e.g., Administrative Reviews, NRC Concerns.
11. Loss of Feedwater e.g., Main Feedwater, Auxiliary Feedwater.
12. Loss of Vital Instrumentation. e.g., Radiation, Pressure, Temperature, & Flow Sensors, Annunciators.
13. Loss of Instrument Air.
14. Mechanical and Seismic Snubber Operation.
15. Spurious Actuations. e.g., Engineered Safety Features, Containment Spray, Recirculation Spray
16. Failure of Charging Pump Event.
17. Failure of Emergency Diesel "Auto" Start.
18. Service Water/Component Cooling Water Heat Exchanger Disruption.
19. Chemistry/Sampling Infractions.
20. Other.

* Identified in draft NUREG-1449

Field 3 - Event Date
mm/dd/yy

Field 3a - Event Time
hhmm (time of action in 24-hour format)

Field 4 - Plant Type/Vendor

1. BWR/GE
2. PWR/W
3. PWR/CE
4. PWR/B&W

Field 5 - Unit Status
LP&S Plant Operational State (POS) immediately prior to event

Field 6 - Noteworthy Plant Conditions
text description with emphasis on unusual equipment and/or plant configurations (not human actions)

Field 7 - Other Unit(s) Status
status of other unit(s) at same site, or "N/A" to represent "no other unit"

Field 8 - Human Action Number & Description
1,2,3... for events with multiple human actions with brief (3-5 word) description of action

Field 9 - Personnel Type

1.   Licensed (Control Room) Operator [PLO]
2.   Non-Licensed (Equipment) Operator [PNO]
3.   Maintenance Technician [PMT]
4.   Contractor/Vendor [PCP]
5.   Utility Management [PUM]
6.   Senior Licensed Operator (Shift Supervisor) [PSO]
7.   Health Physics [PHP]

Field 10 - Event Activity

1.   Administrative [PA]
2.   Construction [PC]
3.   Design [PD]
4.   Fabrication [PF]
5.   Installation or Modification [PI]
6.   Maintenance/Repair [PM]
7.   Operations [PO]
8.   Radiation Protection [PR]
9.   Surveillance Test/Calibration [PT]
10.   Outage Planning/Control [OP]
11.   Outage Management [OM]
12.   Fire Protection [FP]
13.   Fuel Handling & Heavy Load [FH]
14.   On Site Emergency Planning [EP]
15.   Other [PX]

Field 11 - Human Action Location

1.   Control Room
2.   Outside Control Room

Field 12 - System Identification

1. Primary Heat Source Systems
2. Engineered Safety Systems
3. Reactor Auxilliaries Systems
4. Fuel Management Systems
5. Electrical Power Systems
6. Electrical Support Systems
7. Instrumentation and Monitoring Systems
8. Protection and Control Systems
9. Water, Chemical, and Drainage Systems
10. Service Auxilliaries Systems
11. Site Facility Buildings and Structures
12. Power Generation Buildings and Structures
13. Steam Cycle Systems
14. Power Conversion Systems
15. Site Facility Environmental Control Systems
16. Power Generation Buildings Environmental Control Systems
17. Waste Management Systems

Field 13 - Component Identification

1. Accumulators e.g., Gas, Liquid
2. Air/Gas Dryers
3. Batteries
4. Battery Chargers
5. Circuit Closures/Interrupters e.g., Circuit Breaker, Disconnect, Motor/Load Controller, Relays, Switchgear
6. Computers
7. Control Instruments e.g., Flow, Flux, Level, Position, Pressure, Temperature, Velocity, Voltage
8. Control Rods
9. Control Rod Drive Mechanism
10. Demineralizers
11. Eductors e.g., Jet Pump, Steam Jet Air Ejector
12. Electrical Conductors e.g., Insulated Cable, Shielded Cable
13. Electrical Equipment e.g., Amplifier, Converter, Inverter, Rectifier, Transformer, Voltage Regulator
14. Electric Generators e.g., Alternator, Amplidyne, Main Generator, Diesel Generator
15. Electric Heaters
16. Equipment - Nonspecific
17. Fans/Ventilators
18. Filters/Strainers
19. Heat Exchangers e.g., Boiler, Condenser, Cooler
20. Motors e.g., Electric AC, Electric DC, Pneumatic
21. Pipes e.g., Elbow, Nozzle, Reducer/Orifice, Rupture Diaphragm, Tee, Blank Flange
22. Pumps e.g., Centrifugal, Reciprocating, Pump, Rotary, Vacuum
23. Recombiners e.g., Catalytic, Flame, Thermal

Field 13 - Component Identification (continued)

24. Sensors e.g., Conductivity, Current, Flow, Frequency, Flux, Humidity, Level, Position, Pressure, Radiation, Temperature, Velocity, Vibration, Voltage
25. Steam Generators
26. Turbines
27. Valves e.g., Angle, Ball, Check, Diaphragm, Four-Way, Gate, Globe, Needle, Plug, Relief, Three-Way
28. Valve Operators e.g., Electric Motor - AC, Electric Motor - DC, Explosive Squib, Hydraulic, Pneumatic, Solenoid
29. Vessels/Tanks

Field 14 - Displays/Instruments/Controls Identification

1. Qualitative Displays e.g., Annunciator, Computer, Alarm Printer, CRT Text, Indicator Light, Legend Light,
2. Quantitative Displays e.g., Chart Recorder, Computer Printer, Counter - Digital Readout, CRT Alphanumeric Display, CRT Graphic Display, Meter Printing Recorder, Sight Glass (incl. Tygon tube)
3. Two-Position Switches e.g., Keylock, Knob, Multifunction Push-button Matrix, Push-Button (Illuminated Legend), Push-button (Other), Rocker, Toggle Switch/Two Position
4. Multiposition Selectors e.g., J-Handle Switch, Rotary Switch, Stepping Push-button, Toggle Switch
5. Continuously Variable Controls e.g., Knob, Lever, Thumb Wheel,
6. Keyboards e.g., Calculator, Computer Terminal, Teletype, Typewriter
7. Tools e.g., Clippers, Fuse Puller, Impact Wrench, Pliers, Rachet, Screwdriver, Shorting Probe, Torch, Torque Wrench, Welding Rod, Wrench
8. Lifting/Moving Devices e.g., Crane, Come-along, Hoist, Jack, Sling, Wire Rope
9. Electrical Test Equipment e.g., Amprobe, Decade Box, Digital Meter, Frequency Counter, Multimeter, Oscilloscope, Resistance/Impedance Bridge, Signal Generator, Voltage Test Lamp
10. Measurement Test Equipment e.g., Gas Detector, Hydrometer, Micrometer, Thermometer, Scale, Stroboscope, Test Gauge, Vibration Detector
11. Printed Communication e.g., Administrative, Operating, Maintenance, Test or Calibration Procedure, Graph, Label, Log Book, Table, Tag
12. Verbal Communications e.g., Face-to-Face, Page-Party System (PA), Sound-Powered Phone, Telephone, Two-Way Radio
13. Equipment - Nonspecific

Field 15 - Human Action Descriptor

1. Adjust	12. Monitor
2. Allocate Resources	13. Operate
3. Calculate	14. Open/Close
4. Calibrate	15. Organize
5. Check	16. Plan
6. Diagnose	17. Plan
7. Fill/Drain	18. Position
8. Identify	19. Read
9. Inspect	20. Receive
10. Maintain	21. Remember
11. Manage	22. Repair

Field 15 - Human Action Descriptor (continued)

      23. Select
      24. Start/Stop
      25. Test
      26. Use
      27. Verify
      28. Write
      29. Design
      30 Install
      31. Housekeeping
      32. Isolate

Field 16 - Error Mode

0. Unknown
1. Omission
    1.1 omission of task, analysis, or step
    1.2 omission within allotted time
    1.3 omission of alarm response
    1.4 omission of adjustment or calibration
    1.5 other omission human factor
2. Commission
    2.1 commission of undesired task, analysis or step
    2.2 commission of undesired alarm response
    2.3 commission of undesired calibration or adjustment
    2.4 other commission human factor
9. No error (i.e., recovery action)

Classification Scheme

Field 17 - Error Type

0. Unknown
1. Slips
    1.1 correct intention, action not executed as planned
    1.2 inadvertent actuation or disabling of equipment
    1.3 selection of wrong item or failure to follow procedure
2. Mistakes
    2.1 planning inadequate, although action went as planned
    2.2 faulty diagnosis of problem
    2.3 faulty or inadequate procedure
    2.4 incorrect procedure used
    2.5 procedure not used
    2.6 miscommunication
3. Circumventions (actions which contradict procedures)
    3.1   forced - conflicting demands for action results in an action deliberately not performed
    3.2   planned- action taken which deliberately does not follow routine
    3.3   actions taken to gain an advantage in time or in completing requirements, i.e. shortcuts. Examples include performing tests too quickly to finish early, or performing two tests simultaneously
    3.4   reprioritized- priority of activities caused deferment of testing or surveillance

Field 18 - Active/Latent Effect

0. Unknown
1. Active
2. Latent
    2.1 discovered prior to startup
    2.2 discovered during/after startup

Field 19 - Error Influences

1. Procedures
    1.1 Not Used
        1.1.1 no procedure
        1.1.2 not available or inconvenient for use
        1.1.3 procedure difficult to use
        1.1.4 use not required but should be
    1.2 Followed Incorrectly
        1.2.1 format confusing
        1.2.2 more than one action /step
        1.2.3 excess references
        1.2.4 no checkoff
        1.2.5 checkoff misused
        1.2.6 data/computations wrong or incomplete
        1.2.7 graphics LTA
        1.2.8 equipment identification LTA
        1.2.9 ambiguous instructions
        1.2.10 limits LTA
        1.2.11 misuse second check
        1.2.12 details LTA
    1.3 Wrong/Incomplete
        1.3.1 typo
        1.3.2 sequence wrong
        1.3.3 facts wrong
        1.3.4 incomplete/situation not covered
        1.3.5 wrong revision used
        1.3.6 second checker needed

2. Training
    2.1 No Training
        2.1.1 task not analyzed
        2.1.2 decided not to train
        2.1.3 no learning objective
    2.2 Understanding LTA
        2.2.1 learning objective LTA
        2.2.2 lesson plan LTA
        2.2.3 instruction LTA
        2.2.4 practice/repetition LTA
        2.2.5 testing LTA
        2.2.6 continuing training LTA

3. Communications
   3.1 Misunderstood Verbal
      3.1.1 standard terminology not used
      3.1.2 repeat back not used
      3.1.3 long message
      3.1.4 noisy environment
   3.2 No Communication, or Not Timely
      3.2.1 no method available
      3.2.2 late communication
   3.3 Turnover LTA

4. Organizational Factors
   4.1 Standards, Policies, or Admin Controls (SPAC)
      4.1.1 no SPAC
      4.1.2 not strict enough
      4.1.3 confusing or incomplete
      4.1.4 technical error
      4.1.5 drawings/prints LTA
   4.2 SPAC Not Used
      4.2.1 communication of SPAC LTA
      4.2.2 recently changed
      4.2.3 enforcement LTA
      4.2.4 no way to implement
      4.2.5 accountability LTA
   4.3 Management Attention and Oversight
      4.3.1 infrequent audits & evaluations (A&E)
      4.3.2 A&E lack depth
      4.3.3 A&E not independent
      4.3.4 external operating experience LTA
   4.4 Corrective Action
      4.4.1 corrective action LTA
      4.4.2 corrective action not yet implemented
      4.4.3 internal operating experience LTA
   4.5 Employee Communication/Organizational Culture LTA
      4.5.1 employee communications LTA
      4.5.2 no employee feedback
      4.5.3 organizational culture LTA

5. Human Engineering
   5.1 Man-Machine Interface
      5.1.1 labels LTA
      5.1.2 arrangement, placement LTA
      5.1.3 instrument displays LTA
      5.1.4 controls LTA
      5.1.5 monitoring alertness LTA
      5.1.6 unit differences
   5.2 Work Environment
      5.2.1 housekeeping poor
      5.2.2 hot/cold
      5.2.3 bad lights
      5.2.4 noisy
      5.2.5 high radiation/contamination
      5.2.6 cramped quarters
   5.3 Complex System
      5.3.1 knowledge-based decision required
      5.3.2 monitoring more than 3 items at once
   5.4 Non-Fault Tolerant System
      5.4.1 errors not detectable
      5.4.2 errors not recoverable
6. Supervision
   6.1 Preparation
      6.1.1 no preparation
      6.1.2 work package LTA
      6.1.3 pre-job briefing LTA
      6.1.4 walk-through LTA
      6.1.5 tag out LTA
      6.1.6 scheduling LTA
      6.1.7 worker selection
   6.2 Supervision During Work
      6.2.1 no supervision
      6.2.2 LTA supervision
      6.2.3 crew teamwork LTA
7. Stress
   7.1 time pressure
   7.2 fatigue/overtime
   7.3 consequences
8. Engineering Design Change

Field 20 - Recovery Time

xxx (minutes)

Classification Scheme

Field 21 - Recovery Locus

1. Control Room
2. Outside Control Room

Field 22 - Recovery Origin

0. Unknown (U)
1. Skill (S)
2. Rule (R)
3. Knowledge (K)

Field 23 - Related Automatic Equipment Response
    text description

Field 24 - Fission Products Barrier Breached/Threatened

0. Unknown
1. Fuel clad
2. RCS pressure boundary
3. Containment
4. Effluent treatment
9. None

Field 25 - Other Effects
 Text description

Field 26 - Level of Significance

0. Unknown
1. Questionable
2. Detectable
3. Minor
4. Serious

Field 27 - Unique to Low Power or Shutdown

 Y/N

Field 28 - Corrective Action Taken

0. Unknown
1. Operator disciplined, counseled
2. Training program changed
3. Operating procedure modified
4. Administrative procedure modified
5. Operator aids provided
6. Man-machine interface improved
7. Design modification
8. Maintenance procedure modified
9. Surveillance procedure modified
10. Hardware repaired

Field 29 - Event Initiator

Y/N

APPENDIX B

HUMAN RELIABILITY INFLUENCES

DURING LOW POWER AND SHUTDOWN CONDITIONS

IN BWR NUCLEAR POWER PLANTS

M. Donovan[1], J. Forester[2], P. Haas[3], G. Parry[1], D. Whitehead[4]

Project Manager: D. Whitehead[4]

[1]HALLIBURTON NUS Environmental Corp.

[2]Science Applications International Corp.
Albuquerque, NM

[3]Concord Associates

[4]Sandia National Laboratories
Albuquerque, NM

Table of Contents

Table of Contents - continued

Tables

Abbreviations

AEOD	NRC Office for Analysis and Evaluation of Operational Data
AIT	Augmented Inspection Team
AOP	Abnormal Operating Procedures
ASEP HRAP	Accident Sequence Evaluation Program Human Reliability Analysis Procedure
BWR	Boiling Water Reactor
CCW	Component Cooling Water
CDF	Core Damage Frequency
CR	Control Room
CVCS	Chemical Volume and Control System
CRO	Control Room Operators
DHR	Decay Heat Removal
EDG	Emergency Diesel Generator
EOC	Error of Commission
EOM	Error of Omission
EOP	Emergency Operating Procedure
EPRI	Electric Power Research Institute
ES	Engineered Safeguards
ESFAS	Engineered Safety Features Actuation System
ESW	Emergency Service Water
GGNS	Grand Gulf Nuclear Station
HACS	Human Action Classification Scheme
HPIP	Human Performance Investigation Process
HRA	Human Reliability Analysis (or Assessment)
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
IAE	Instrumentation and Electronics
IIT	Incident Investigation Team
INPO	Institute of Nuclear Power Operations
LER	Licensee Event Report
LOCA	Loss of Coolant Accident
LP&S	Low Power and Shutdown
LPI	Low Pressure Injection
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission (or U.S. NRC)
NUCLARR	Nuclear Computerked Library for Assessing Reactor Reliability
NUMARC	Nuclear Utility Management and Resources Council
NSAC	Nuclear Safety Analysis Center
NSO	Nuclear Station Operator
POS	Plant Operational State
PRA	Probabilistic Risk Assessment
PWR	Pressurked Water Reactor
PZR	Pressurker
RAT	Reserve Auxiliary Transformer
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RHRS	Residual Heat Removal System
RO	Reactor Operator
RV	Reactor Vessel

SCRE   Shift Control Room Engineer
SCSS   Sequence Coding and Search Scheme (for LERs)
SDC   Shutdown Cooling
SE   Shift Engineer
SFP   Spent Fuel Pool
SLIM/MAUD Success Likelihood Index Methodology/Multi-Attribute Utility Decomposition
THERP Technique for Human Error Rate Prediction
TS   Technical Specifications

B.1. INTRODUCTION

B.1.1 Background

Recent incidents at U.S. nuclear power plants [e.g., NRC, NUREG-1410] and resulting NRC studies of Low Power and Shutdown (LP&S) operations [e.g, NRC, NUREG-1449] have suggested that the LP&S operating environment creates a set of circumstances that are unique in their contribution to human performance and reliability. Given this is the case, it is likely that the conventional approaches used for assessing human reliability in nuclear power plants may be inadequate for LP&S and that a more refined methodology will be required.

In this context, the NRC has undertaken an effort to conduct a comprehensive human reliability analysis (HRA) during LP&S conditions. The objectives of the comprehensive HRA project are to: (1) identify the factors that contribute to human performance during LP&S conditions; (2) select a methodology for performing an assessment of human reliability that takes into account the unique characteristics of plant operations during LP&S; and (3) estimate the contribution of human performance to plant risk during LP&S and the uncertainties associated with that estimate.

Sandia National Laboratories (SNL) was tasked with conducting the comprehensive HRA analysis for boiling water reactors (BWRs), while Brookhaven National Laboratory (BNL) was made responsible for the analysis in the context of pressurized water reactors (PWRs). SNL and BNL were to collaborate whenever possible in order to avoid unnecessary duplication of effort. This appendix documents the results of the first phase of the NRC comprehensive HRA project conducted by Sandia National Laboratories. Specific areas of collaboration between SNL and BNL are noted as well.

B.1.2 Objective

The objective of this phase of the comprehensive HRA project was to identify the unique characteristics, performance influencing factors, and classes of errors which must be considered in selecting a methodology for HRA of LP&S conditions.

B.1.3 Approach

Three major tasks were undertaken to accomplish the above objective. First, recent NRC and industry reports of investigations and studies related to LP&S operations were reviewed. The primary goal of the literature review was to identify factors and characteristics that are unique to the LP&S environment in their contribution to human performance and reliability.

Second, a review of Licensee Event Reports (LERs) was conducted to identify and characterize the more critical types and/or classes of human errors that occur during LP&S and to identify their potential causes or influencing factors. A human action taxonomy or classification scheme was developed jointly by SNL and BNL to facilitate the extraction of the relevant information from the LERs. A total of 555 LER events from ten different BWRs were reviewed by SNL and a data base containing the relevant information was created and analyzed.

Finally, a series of interviews were conducted with personnel from the NRC, the Electric Power Research Institute (EPRI), the Nuclear Management and Resources Council (NUMARC) and two nuclear power plants (a BWR and a PWR) who were knowledgeable in LP&S operations and controls. The goal of the interviews was to obtain supporting and additional information regarding the activities, operations, situations, human tasks and performance influencing factors that should be considered in the development of a comprehensive HRA model for LP&S operations. Interview protocols were developed jointly by SNL and BNL team members for use with utility and non-utility personnel. The interview protocols were developed in order to allow the needed information to be obtained in a consistent and systematic manner. Non-utility interviews were conducted by joint SNL and BNL

teams. PWR plant personnel were interviewed by BNL team members, while BWR personnel were interviewed by the SNL team.

B.2. REVIEW OF REPORTED EVENTS AND ASSOCIATED STUDIES AND CLASSIFICATION OF EVENT-SPECIFIC DATA

B.2.1 Introduction

This section documents the methods and results of the LER and literature reviews. As noted above, in order to allow a systematic characterization of the data contained in the LERs, a human action classification scheme (HACS) was developed jointly by SNL and BNL. The development of the classification scheme is discussed in Section B.2.2.

A detailed discussion of the methodology used in the LER review and identification of the reports selected for review are presented in Section B.2.3. The results of the LER review are presented and discussed in Section B.2.4.1, with the reviews of relevant literature following in Section B.2.4.2.

B.2.2 Classification Scheme Development

In order to classify and characterize the types of human errors occurring during LP&S and identify the more critical performance influencing factors, a classification scheme was developed using a variety of information sources and existing instruments, including:

- NUREG-1449 - *NRC Evaluation of Shutdown and Low Power Operation*, Jan. 24, 1992.

- NUREG/CR-3905 - *Sequence Coding and Search System for Licensee Event Reports*, Aug. 1984.

- *IEEE Recommended Practice for System Identification in Nuclear Power Plants and Related Facilities, Table 1*, IEEE Standard 805 - 1984.

- NUREG/CR-4639 - *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR)*, Vol. 4, 1990.

- NUREG/CR-5455 - *Human Performance Investigation Process (HPIP)*

- J. Reason, *Human Error*, Cambridge University Press, 1990.

The resulting human action classification scheme (HACS) was used to systematically code the relevant information contained in the LERs for placement in a data base. A condensed version of HACS is presented in Appendix A.

B.2.3 Sources of Information Reviewed

B.2.3.1 Sources of Information and Methodology for LER Review

The goal of the Licensee Event Report (LER) review was to identify and classify the kinds of human errors occurring during LP&S conditions and to determine the dominant factors contributing to the occurrence of those errors. In order to accomplish this goal,
relevant LER summaries were obtained from the Sequence Coding Search System (SCSS) program operated by Oak Ridge National Laboratory for the Nuclear Regulatory Commission (NRC). The SCSS program maintains a computerized database of event report summaries that are coded in order to allow retrieval and/or representation of the summaries according to selected criteria. The search conducted for the present study located LERs according to the following criteria:

- Events occurring at BWR plants with the unit operating at or below 15% power.
- Events occurring between 1980 and November, 1991
- Events in which one or more personnel errors were reported.

The search identified 4,814 events. On the basis of a similar search that retrieved all LER summaries from BWRs with the unit operating at or below 15% power (7,382 events), events reporting personnel errors constituted approximately 65% of the LP&S related events.

Ten plants were selected to provide a representative sample of LERs from United States BWRs. The plants were selected so that the sample represented the different types of BWRs and containments (which correlate with plant age), and the relative frequency of occurrence of the different types in the U.S. The plants selected were:

- Oyster Creek   BWR 2, Mark I
- Dresden 3   BWR 3, Mark I (Isolation Condenser)
- Quad Cities   BWR 3, Mark I
- Vermont Yankee   BWR 4, Mark I
- Peach Bottom 2   BWR 4, Mark I
- Susquehanna 1   BWR 4, Mark II
- WNP 2   BWR 5, Mark II
- LaSalle 1   BWR 6, Mark II
- Grand Gulf   BWR 6, Mark III
- River Bend   BWR 6, Mark III

A total of 555 human actions were reviewed and coded into the data base from the LERS. Although no systematic training or procedures for using HACS were provided, coding strategy was discussed among the team members at several points during the task to help attain some level of consistency. However, since no measure of inter-rater consistency was obtained, the results of the LER review should be considered preliminary. Additional research will be necessary before the numerical data can be taken as more than approximations.

Not all LERs reviewed for the ten plants were coded into the data base. Some selection of LERs for coding was done on the basis of coder judgement concerning relevance of the event for study. For example, an LER reporting a Technical Specification violation for failing to post a timely fire watch may not have been coded. The data base contains only events for which complete coding was attempted. For most of the plants, at least the last 5 years of LERs were reviewed, with ten years of LERs reviewed for some plants.

B.2.3.2   NRC and Industry Documents Reviewed

In order to identify and evaluate the unique issues, factors, and salient features of LP&S operations relevant to human performance and reliability, several recent documents related to LP&S environments were reviewed. The documents included the following:

- NUREG-1410 - *Loss of Vital AC Power and the Residual Heat Removal System During Mid-Loop Operations at Vogtle Unit 1 on March 20, 1990.*

- NUREG-1449 - *NRC Evaluation of Shutdown and Low Power Operation*, Jan. 24, 1992.

- SECY-91-283 - *Evaluation of Shutdown and Low Power Risk Issues*, Sept. 9, 1991.

- NSAC/157 - *Residual Heat Removal Experience Review and Safety Analysis, Boiling Water Reactors, 1984-1989*, June 1991.

- NUMARC 91-06 - *Guidelines for Industry Actions to Assess Shutdown Management*, Dec. 1991.

Each of the reports is reviewed and discussed in Section B.2.4.2 with the goal of illuminating the unique aspects of LP&S conditions which will impact the assessment of human performance and reliability.

B.2.4   Results and Discussion of Reviews

B.2.4.1   Results and Discussion of LER Review

Initial summary statistics for the results of the LER review are presented in Table B.1. The percentages in the table reflect the number of times out of 555 human error events that an identified human action was indicated as falling into a particular category. In some cases, the results from a particular category were broken down by sub-categories. For example, the results from Field 18 indicated that 38.9% of the identified human errors had latent effects. That is, the identified errors did not have an immediate, noticeable effect on plant functioning. The results of the sub-category breakdown of the identified latent errors indicated that 35.6% were discovered prior to reactor startup, with 41.2% discovered during or after startup. For the present analysis, sub-category breakdowns were done only for selected categories (see HACS, Appendix A, for possible additional sub-category breakdowns).

In examining the results of the LER review, it should be kept in mind that the findings are only preliminary. Without systematic training and detailed procedures for the individuals responsible for coding the data, low inter-rater reliability is possible. Thus, the percentages listed below should not be considered to be more than approximations. However, given the absence of other data, the results of the LER review can serve as an initial guide for where and what kinds of errors to model in a LP&S PRA.

Table B.1 Initial Summary Statistics for SNL Licensee Event Report Review

Field 2 - Event Description Summary

Category	Percentage
Loss of SDC (Predominantly RHR cooling losses)	10.8%
Loss of Reactor Coolant Inventory	2.7%
Loss of Electrical Power	6.3%
Quality Assurance Inspections and Infractions (Predominantly 10 CFR Infractions/Tech. Spec Violations)	21.4%
Loss of Vital Instrumentation	2.3%
Spurious (Inadvertent) ESF Actuation	27.2%
Other/unknown	18.7%
Remaining Categories Together (14) (None of the other potential events occurred more than 2% of the time)	10.4%

Field 5 - Unit Status

Category	Percentage
Extended outage	1.6%
Routine Start-up	17.4%
Routine Shutdown	2.0%
Steady State Operation	2.7%
Load Change During Routine Power Outage	----
Refueling	41.1%
Cold Shutdown	25.9%
Hot Shutdown	6.3%
Hot Standby	0.2%
Unknown	2.7%

Field 7 - Other Unit Status

Approximately 93% the responses indicated either "no other unit" or "other unit status unknown."

Field 9 - Personnel Type

Category	Percentage
Licensed Control Room Operator	25.6%
Non-Licensed Operator	7.4%
Maintenance Technician	32.7%
Contractor/ Vendor	14.2%
Utility Management	2.3%
SRO (Shift Supervisor)	1.4%
Health Physics	1.4%
Other/Unknown	14.8%

Table B.1 Initial Summary Statistics for SNL Licensee Event Report Review (Continued)

Field 10 - Event Activity

Category	Percentage
Administrative	3.1%
Construction/Fabrication	2.7%
Design	6.0%
Installation or Modification	8.3%
Maintenance/Repair	18.7%
Surveillance Test/Calibration	32.1%
Operations	18.9%
Outage Planning/Control/Management	2.0%
Fire Protection	1.1%
Fuel Handling & Heavy Load	1.3%
Other/Unknown	4.9%
Remaining Categories Together (2)	0.9%

Field 11 - Human Action Location

Category	Percentage
Control Room	26.7%
Outside Control Room	64.9%
Other/Unknown	8.5%

Field 12 - System Identification

Category	Percentage
Primary Heat Source Systems	6.1%
Engineered Safety Features	15.1%
Reactor Auxiliary Systems	6.5%
Fuel Management Systems	1.6%
Electrical Power Systems	18.2%
Instrumentation and Monitoring	10.1%
Protection and Control Systems	19.1%
Steam Cycle Systems	6.7%
Power Generation Buildings	3.6%
Other/unknown	5.0%
Remaining Categories Together (8)	9.5%

Field 13 - Component Identification

Category	Percentage
Circuit Closures/Interrupters (Predominantly circuit breakers, relays, and switches)	25.0%
Sensors (Predominantly radiation, flux, temperature, and level)	15.0%
Valves	13.3%
Pumps	5.2%
Electrical Conductors	4.3%
Control Instruments	4.0%
Equipment- Nonspecific	8.6%
Unknown	10.6%
Remaining Categories Together (22)	14.2%

Table B.1 Initial Summary Statistics for SNL Licensee Event Report Review (Continued)

Field 14 - Displays/Instruments/Controls Identification

Category	Percentage
Printed Communication (Predominantly Administrative, Maintenance, or Test/Calibration Procedure)	23.2%
Qualitative Displays (Annunciators, Indicator Lights)	8.8%
Equipment-Nonspecific	7.9%
Tools	5.0%
Quantitative Displays	4.7%
Multiposition Selectors	4.5%
Unknown	39.5%
Remaining Categories Together (4)	6.3%

Field 15A - Human Action Descriptor

Category	Percentage
Test	21.8%
Operate	13.9%
Maintain	10.8%
Install	7.7%
Design	6.7%
Repair	5.8%
Calibrate	4.3%
Open/Close	4.3%
Unknown	3.6%
Remaining Categories Together (22)	21.8%

Field 15B - Human Action Descriptor - NUCLARR Level 1

Category	Percentage
Maintenance Technician - Maintain	16.9%
Maintenance Technician - Test	12.4%
Control Room Operator - Operate	12.4%
Control Room Operator - Test	5.0%
Control Room Operator - Monitor	4.1%
Unknown	38.6%
Remaining Categories Together (8)	10.4%

Field 15C - Human Action Descriptor - NUCLARR Level 2

Category	Percentage
Maintenance Technician - Test	11.5%
Maintenance Technician - Maintain	7.9%
Maintenance Technician - Repair	7.4%
Control Room Operator - Operate	7.0%
Control Room Operator - Monitor	4.7%
Control Room Operator - Open/Close	4.7%
Maintenance Technician - Calibrate	7.4%
Unknown	43.9%
Remaining Categories Together (10)	9.6%

Table B.1 Initial Summary Statistics for SNL Licensee Event Report Review (Continued)

Field 15D - Human Action Descriptor - NUCLARR Level 3

Category	Percentage
Use	10.1%
Position	9.2%
Monitor	4.0%
Maintain	3.2%
Select	2.3%
Unknown	62.7%
Remaining Categories Together (10)	8.5%

Field 16 - Error Mode

Category	Percentage
Omission (Percentage of Total)	29.5%
Sub-categories of omissions (percentages are of total omissions)	
Omission of task, analysis, or step	62.1%
Omission within allotted time	22.0%
Omission of alarm response	0.6%
Omission of adjustment or calibration	4.3%
Other omission human factor	5.5%
Other	5.5%
Commission (Percentage of Total)	60.9%
Sub-categories of commissions (percentages are of total commissions)	
Commission of task, analysis, or step	87.6%
Commission of undesired alarm response	0.6%
Commission of undesired adjustment. or calibration	3.6%
Other commission human factor	5.0%
Other	3.3%
Unknown	6.7%
No Error	2.9%

Field 17 - Error Type

Category	Percentage
Unknown	26.3%
Slips	35.0%
Sub-categories of Slips (percentages are of total slips)	
Correct intention, action not executed as planned.	24.3%
Inadvertent actuation or disabling of equipment	45.4%
Selection of wrong item or failure to follow procedure	27.8%
Sub-category not specified	2.6%

Table B.1 Initial Summary Statistics for SNL Licensee Event Report Review (Continued)

Mistakes	36.6%
Sub-categories of Mistakes (percentages are of total mistakes)	
Planning inadequate, although action went as planned	26.6%
Faulty diagnosis of problem	7.4%
Faulty or inadequate procedure	39.4%
Incorrect procedure used	4.4%
Procedure not used	10.3%
Miscommunication	6.7%
Sub-category not specified	4.9%
Circumventions	2.2%

Field 18 - Active/Latent Effect

Category	**Percentage**
Unknown	7.2%
Active	53.9%
Sub-categories of Active (percentages are of total active effects)	
Initiating event related	73.2%
Response related	1.7%
Not specified	25.0%
Latent	38.9%
Sub-categories of Latent (percentages are of total latent effects)	
Discovered prior to startup	35.6%
Discovered during/after startup	41.2%
Not specified	23.1%

Field 19 - Error Influences

More than one Error Influence could be indicated for a given event. Category percentages reflect the number of times the category was selected on the 555 data sheets. Sub-category percentages reflect the percentages within the category.

Category	**Percentage**
Unknown	23.8%
Procedures	47.2%
Not used	13.4%
Followed incorrectly	32.1%
Wrong/incomplete	54.6%
Training	14.2%
No training	12.6%
Understanding less than adequate (LTA)	82.3%
Communications	4.7%
Organizational Factors	13.3%
Inadequate Standards, Policies, or Administrative Controls (SPAC)	71.6%
SPAC not used	10.8%
Management attention and oversight	12.2%
Corrective action inadequate	4.1%

Table B.1 Initial Summary Statistics for SNL Licensee Event Report Review (Continued)

Human Engineering	16.2%
Man-machine interface	61.1%
Work environment	15.6%
Complex systems	11.1%
Non-fault tolerant systems	6.6%
Supervision	11.3%
Inadequate preparation prior to work	57.1%
Inadequate supervision during work	40.0%
Stress	0.0%
Engineering Design Change	1.6%

Field 21 - Recovery Locus

Category	Percentage
Unknown	16.6%
Control Room	29.6%
Outside Control Room	53.7%

Field 22 - Recovery Origin

Category	Percentage
Unknown	29.3%
Skill	9.7%
Rule	44.5%
Knowledge	16.4%

Field 24 - Fission Products Barrier Breached/Threatened

Category	Percentage
Unknown	9.9%
None	78.7%
Fuel clad	7.7%
Other categories together	7.2%

Field 27 - Unique to Low Power or Shutdown

Category	Percentage
Unknown	3.2%
Yes	46.1%
No	50.6%

Review

Table B.1 Initial Summary Statistics for SNL Licensee Event Report Review (Continued)

<u>Field 28 - Corrective action Taken</u>

<u>Category</u>	<u>Percentage</u>
Unknown	38.4%
Operator disciplined/counseled	6.5%
Training program changed	4.3%
Operating procedure modified	8.5%
Administrative procedure modified	8.1%
Operator aids provided	0.7%
Man-machine interface improved	3.2%
Design modification	11.6%
Maintenance procedure modified	3.4%
Surveillance procedure modified	9.9%
Hardware repaired	11.3%

Note: Procedure modifications of some sort constituted 30% of the corrective actions.

Highlights of the initial breakdowns displayed in Table B.1 in regard to human reliability during LP&S are presented below. Many of the findings provide guidance for where HRA analysts should focus their attention in modeling human errors during LP&S. Highlights included:

- 10.8% of the events are coded as a loss of shutdown cooling. For the 61 calendar years of LERs reviewed, this represents a human-induced initiating event frequency of 0.98 events/ calendar year for loss of shutdown cooling, which is significant from the at-power operations perspective and deserves further examination.

- The derived human-induced initiating event frequencies for loss of reactor coolant inventory and for loss of electrical power are 0.24 events/calendar year and 0.57 events/calendar year, respectively.

- Not surprisingly, maintenance/test/repair activities account for the highest proportion of errors. Operations activities only account for 18.8% of the errors.

- The greatest number of errors are concentrated in four systems groups: Protection and Control, Electric Power, Engineered Safety, and Instrumentation and Monitoring.

- 25% of the errors occur during personnel interactions with circuit closures/interrupters, with 15% occurring during interactions with sensors.

- 60.9% of the identified errors are classified as Errors of Commission (EOCs), compared to 29.5% classified as Errors of Omission (EOMs). Since primarily EOMs are modeled in full-power PRAs, these results may indicate a greater need to include an examination of EOCs during LP&S studies (at least for pre-accident events). This idea is discussed further below.

- Slips (i.e., the individual had a correct intention, but committed an inadvertent action) occur about as frequently as mistakes (i.e., the individual did what he/she intended, but it was an incorrect intention).

- 53.9% of the errors have active as opposed to latent effects (38.9%). More latent errors were discovered during or after startup (41.2%), than prior to startup (35.6%).

- Procedures were the most frequently cited error influencing factor.

The results presented in Table B.1 provide a general picture of the kinds of human errors and their influences which occur during LP&S. In order to obtain more refined information about some of the more important aspects of LP&S, several of the event categories were examined as function of their relationship with other categories. Some of the more interesting summary results from this analysis are presented below:

- Loss of Shutdown Cooling (60 events)

    - 58.3% of the loss of shutdown cooling (SDC) events occur during refueling

    - 40.0% of the human errors involve maintenance technicians, while 28.3% are accounted for by control room operators.

    - 61% of the loss of SDC events involve test, calibration, maintenance, repair, or installation. Only 16.6% are related to operations activities.

    - 33.3% of errors relate to work with the Electrical Power Systems, 21.6% with Engineered Safety Systems and 16.6% with Reactor Recirculation System.

    - 81.7% of the loss of SDC events involve errors of commission. Slips

and mistakes involve approximately equal proportions.

- 83.3% of the loss of SDC errors have active effects.

- Procedures were cited as a PSF in 50% of the errors associated with a loss of SDC. Supervisor was cited 40.0% of the time, training 30.0%, human engineering 18.3%, and oranizational factors 16.6% of the time.

• Loss of Electrical Power (35 events)

- 37.1% of the loss of electrical power events occur during refueling, with the same percentage (37.1%) occurring during cold shutdown.

- 37.1% of errors resulting in a loss of electrical power involve maintenance technicians, while 17.2% are related to actions by control room operators.

- 62% of the loss of power errors involve test, calibration, maintenance, repair, or installation. Only 14.2% relate to operations actions.

- 94.3% of the loss of power errors relate to work with the Electrical Power Systems,

- 68.6% of the loss of power errors are identified as errors of commission. Most of the losses of electrical power occur due to slips (45.7%) as opposed to mistakes (22.9%).

- 71.4% of the errors related to loss of electrical power have active effects.

- Procedures are cited as a PSF in 37% of the errors associated with a loss of power. Supervision was cited 17% of the time, training 17%, human

engineering 20%, and organizational factors 17%.

- Only 20% of the loss of Electrical Power events are categorized as unique to LP&S.

• Error Mode by Personnel Type

- Licensed Control Room Operators (LCROs) are responsible for a greater percentage of the errors of omission (32.3%) than are the maintenance technicians (25%). Conversely, maintenance technicians commit more of the errors of commission (37.9%) than do the LCROs (23.4%).

- Contractors/Vendors account for 18% of the EOCs, but are responsible for only 7.3% of the EOMs.

- Nevertheless, all personnel are more likely to commit an EOC than an EOM.

• Error Mode by Error Type

- Of the EOCs, 45% are slips, while 33% are mistakes.

- Of the EOMs, 28% are slips, while 54% are mistakes.

• Error Mode by Error Effect

- Of the EOCs, 63% have an active effect, with 32% having latent effects.

- Conversely, of the EOMs, only 33% have an active effect, while 56% have a latent effect.

The results described above highlight some of the more interesting relationships among the different classifications and provide at least some initial insights into the nature of the human errors occurring during LP&S. These findings provide

direction for the initial focus of a PRA addressing LP&S. For example, while EOCs apparently occur more frequently than EOMs and should certainly be given additional attention (relative to full-power) during LP&S, it may be the case the EOMs are of greater concern. The results suggest that EOMs are more likely to reflect a mistaken intention than a slip and are also more likely to have latent effects than active effects. If it is argued that latent errors and errors that occur because of a misunderstanding of the situation have a greater potential for causing difficult-to-recover problems, then it would be a mistake to concentrate heavily on EOCs at the exclusion of EOMs. Obviously, the extensiveness of the classification scheme that is used to code the LER data provides the opportunity for many additional breakdowns that may be relevant to developing an HRA methodology specific to LP&S.

B.2.4.2   Literature Reviews

B.2.4.2.1   Loss of Vital AC Power and the Residual Heat Removal System During Mid-Loop Operations at Vogtle Unit 1 on March 20, 1990, NUREG-1410, June 1990

The loss of vital AC power and resulting events which occurred at the Vogtle Nuclear Plant during mid-loop operations revealed a number of important human performance and reliability issues relevant to LP&S conditions and to plant operations in general.

The initial human error in the Vogtle incident occurred when a fuels and lubricants truck in the low voltage switchyard was inadvertently backed into the support column for an offsite power feed to the reserve auxiliary transformer, which was supplying safety power. The result was a phase-to-ground fault and the opening of the feeder breakers for the safety buses. Following the loss of the one in-service reserve auxiliary transformer, the one operable emergency diesel generator malfunctioned. With the loss of all safety bus AC power, the Residual Heat Removal System was not available.

Although the driver of the fuels and lubricants truck had performed the duties of refueling air

compressors and welding machines in the switchyard on an irregular basis for about a year, the absence of temporary equipment usually located in the switchyard led the driver to pull straight in, as opposed to backing in as he usually did. As prescribed by procedures, the driver was accompanied by a security escort. However, the driver was not aware that plant safety standards required a ground guide when the rear view of a vehicle was blocked and had not received any training in this regard.

The report concluded that the "Vogtle staff had inadequate control of switchyard activities" and that "guidance identifying the need for additional controls and precautions for work on electrical equipment, including work in the switchyard, had previously been provided to the industry."

An implication of the above findings is that the Vogtle staff was limited in their ability to respond to available guidance and that "programmatic deficiencies" may have existed in the sense that the plant had not established sufficient programs to respond to guidance and help protect the plant during LP&S conditions. While the human error associated with the loss of AC power at Vogtle could conceivably have occurred at anytime, the related events that followed point out the importance of well-structured outage planning and support for critical human actions.

Emergency Diesel Generator Malfunction

As noted above, with the loss of offsite power, the one operable emergency diesel generator (EDG) malfunctioned. Specifically, the 1A EDG started automatically, carried its loads for 80 seconds, and then tripped. Approximately 18 minutes later, it was restarted and carried its loads for 70 seconds before tripping again. Operators failed to correctly diagnose the reasons for the trips and were thereby limited in their ability to respond to the problem. After another 15 minutes (36 minutes into the incident), the emergency diesel generator was again started using a manual emergency start rather than a normal under-voltage start. With this start, the generator continued to run and carry its loads

without incident. (The actual cause of the trips had not yet been definitely determined when the report was published.)

While the Technical Specifications allowed having only two sources of AC power in service during cold shutdown, the report noted that it may not be prudent during mid-loop operations and that "Vogtle made no attempt in their outage planning to shift this configuration to a less sensitive time during the outage." This circumstance points out the potential limitations of current Technical Specifications for LP&S conditions and the additional burdens placed on operators to determine inappropriate LP&S configurations.

Regarding the operators' handling of the EDG failure, the report noted that the operators had developed a tendency to automatically press the acknowledge button and then the reset button to clear spurious and other nuisance alarms before identifying the cause of the alarm. This tendency led the control room operators to acknowledge and reset the EDG annunciator for the first trip without noting or recording what tripped the EDG. A plant operator sent to check the diesel also cleared and reset the alarms at the EDG without recording what alarms occurred. While this tendency has obvious drawbacks, it is not clear that noting the alarms would have made a difference since multiple annunciations had occurred and would not necessarily have narrowed the problem. Clearly, serious limitations existed in the human-machine interface in regards to diagnosing the EDG faults. Nuisance alarms were a major problem.

Furthermore, although the operators did attempt to attend to the alarms etc., at the second EDG trip, they were not aware of the "first out" feature of the alarm system. The "first out" feature is intended to make it possible to determine which of the annunciators first indicated a problem. However, further confounding the problem was the fact that the "first out" feature for the EDG alarm system was not functioning correctly. If the operators had been aware of the first out feature and relied upon it the way it was malfunctioning, it is possible that they may have delayed or even failed to try the

manual start approach. They tried the manual start because they thought certain trip signals would be bypassed and they were correct.

In the report, it was also noted that the visual design of the panels did not help operators to rapidly diagnose the cause of the trips. Moreover, it was determined that some of the plant operators were not aware that the sequence in which they respond to annunciators is critical and that variations in the sequence can cause "alarm sequences to appear to operate strangely." Clearly, limitations in the human-machine interface and the design of appropriate procedures and safeguards to deal with the situation had not been adequately addressed by the plant prior to the incident. While the human and machine limitations in diagnosing and responding to the EDG failure are not strictly tied to LP&S, the unique configurations and circumstances of shutdown emphasize the importance of adequate personnel training and good human factors design.

Establishment of Bus Cross-ties to Restore Power

During the incident, personnel assigned to determine ways to establish bus cross-ties to restore power failed to recognize potential problems and limitations created by the shutdown conditions. It was noted in the report that the Vogtle loss of AC power procedures did not address shutdown conditions and were of little help during the incident. This finding emphasizes the importance of developing procedures specific to shutdown conditions. It also emphasizes the importance of developing a process or methodology to identify critical human actions during shutdown conditions and then reducing the likelihood of error by developing appropriate procedures. Finally, an absence of adequate procedures under LP&S conditions creates the potential for a variety of operator responses to unusual circumstances (i.e., errors of commission), and makes modeling human reliability during LP&S conditions quite different than during power operating modes.

Miscommunications Resulting in Delays and Error

Due to miscommunication and shortcomings in coordination, several delays and an important error occurred in closing the Reactor Coolant System boundary after the loss of power. The time to "button up" the steam generator manways was lengthened due to unclear directions on the removal of personnel from the containment building. This confusion led to personnel being taken off and then returned to the job. In addition, the pressurizer manway was incorrectly closed due to miscommunication.

The report concluded that the effects of communication problems and coordination shortfalls are more pronounced during an incident where several maintenance activities are already underway (e.g., during LP&S). In this incident it appears that some individuals who were in the communication sequence probably should not have been because they were not knowledgeable enough to be able determine the correct action in the face of conflicting instructions. For example, the manager of Health Physics and Chemistry was relaying instructions regarding the RCS boundary closing and was apparently unaware of the importance of the pressurizer manway remaining open. The frequency of these kinds of human errors can only be reduced by planning an appropriate communication structure for LP&S conditions.

Other Human Errors

In addition to the human errors discussed above, the Vogtle report identified the potential for other human errors based on inadequate procedures, inadequate training, and shortcomings in human-machine interface factors such as labelling and display design. Many of the issues raised in the report are specifically tied to the need for better planning and procedures for dealing with low power and outage conditions. A sampling of the potential problem areas include:

- Inadequate procedures for loss of the Residual Heat Removal System, particularly during mid-loop operations.

- Inadequate procedures for loss of AC power.

- Inadequate procedures and training for diesel generator operations, particularly in responding to lockout of a diesel generator following shutdown.

- No procedures or training for Reactor Coolant System Configuration Control.

- Inadequate training and procedures for understanding shutdown thermal-hydraulic phenomena and behavior.

- Inadequate procedures for expedited closure of the containment building equipment hatch.

- Possible inadequacies in procedures for evacuation and accountability of on-site personnel for emergencies during outages.

- Insufficient labelling at load sequencer panels and inadequate design of annunciator panels and controls.

As noted earlier, an absence of adequate procedures creates the potential for a variety of operator responses to unusual circumstances (i.e., errors of commission) and makes modeling human reliability during LP&S conditions quite different than during power operating modes. The problem areas listed above indicate that the situation is magnified when inadequate training has been given and information displays are insufficient.

B.2.4.2.2   NRC Evaluation of Shutdown and Low Power Operation, NUREG-1449, January 24, 1992

The evaluation described in NUREG-1449 was initiated following the NRC staff's investigation of the loss all vital AC power during a shutdown on March 20, 1990 at the Vogtle Nuclear Plant. The goal of the evaluation was to provide a broad assessment of risk during shutdown, refueling, and startup. A number of technical studies were completed as part of the evaluation and the results

of the studies are summarized in the report. The studies include:

- A systematic review of operating experience during hot and cold shutdown and refueling.

- An analysis of a spectrum of events to estimate the conditional probability of core damage using the Accident Sequence Precursor (ASP) analysis methodology.

- Site visits and interviews regarding shutdown practices.

- Reviews and evaluations of existing shutdown- related PRAs.

- Compilations and reviews of existing regulatory requirements for shutdown operation.

- Thermal-hydraulic analyses to estimate the consequences of extended loss of Residual Heat Removal (RHR) and use of alternate methods of RHR.

- Preliminary Level 1 PRAs for LP&S operating modes for a pressurized-water reactor (PWR) and a boiling-water reactor (BWR).

<u>Comprehensive Results</u>

On the basis of these analyses of LP&S conditions, a number of important technical issues relevant to the LP&S environment were identified. Five issues determined to be especially important included:

- Outage planning and control;

- Stress on personnel and programs;

- Training and procedures;

- Technical specifications; and

- PWR safety during midloop operation.

The first four of these issues have particular relevance to human reliability. First, outage planning and control is critical due to the wide diversity of activities to be accomplished, the concurrent performance of multiple maintenance activities, the increased numbers and types of personnel working in the plant, the limited technical specification controls which exist during LP&S conditions, and the often unexpected problems and delays that occur. Not only do these factors have the potential for increasing the probability of human error relative to full-power modes, but the potential for human error also arises in the actual planning and control activities. Careful scheduling and good communication and coordination play a major role in avoiding human actions that could place the plant in situations likely to challenge safety functions.

Second, because of the variety of activities, the rapid changes in plant configurations, the often tight scheduling and a general rush to complete the outage, stress levels on personnel can increase dramatically and remain high over fairly long periods of time. In addition, inappropriate use of overtime has been observed which can further compound the problem.

Third, the training of licensed personnel to perform shutdown operations has generally not been emphasized. Training with simulators for shutdown conditions is not common, and more importantly, training for actions outside the control room that may be required to mitigate shutdown events has not been as extensive. Further compounding the problem are non-existent or potentially inadequate plant procedures for dealing with many possible shutdown events.

Finally, the report indicated that technical specifications for residual heat removal (RHR) systems, emergency core cooling systems (ECCS), containment systems and electrical systems were not detailed enough to address the number and risk significance of system configurations used during LP&S conditions. With these deficiencies, the burden on plant personnel to recognize risky plant configurations is increased along with the potential for human error.

The above issues strongly indicate that LP&S conditions create a very different environment for human task performance than that in full-power modes. In addition to these general influences on human performance noted above, the report discusses a number of more specific issues related to LP&S conditions that bear on plant safety and that may have important relationships with human performance. These topics include:

- instrumentation deficiencies;

- loss of residual heat removal capability;

- containment capability;

- rapid boron dilution;

- fire protection;

- ECCS recirculation capability;

- onsite emergency planning;

- fuel handling and heavy loads;

- potential for draining the BWR reactor vessel; and

- inspection programs.

Specific Findings From Selected Studies

Several of the studies reviewed in NUREG-1449 contained results which particularly pointed out the uniqueness and criticality of the human role during LP&S conditions. The studies included the review of operating experience, the Accident Sequence Precursor analysis conducted by the NRC Office for Analysis and Evaluation of Operational Data (AEOD), and the NRC assessment of shutdown operations through site visits and systematic observations.

The AEOD assessment of plant operating experience revealed several classes of critical events with important human error contributions. The results of the study indicated the following:

- Sixty percent of the BWR and PWR loss of shutdown cooling events reviewed were caused by human error.

- Loss of reactor coolant events tended to be caused by valve lineup errors. Of 12 BWR events reviewed, ten were caused by human error. Six of ten of the PWR events reviewed were human caused.

- Of eight breach of containment events (BWR & PWR), all were caused by human error.

- Twenty of the loss of power events reviewed in BWRs were caused by human error, while 5 out of 11 were human error related in PWRs.

- Significant numbers of overpressurization events, flooding and spill events, and inadvertent reactivity addition events were caused by human errors.

The Accident Sequence Precursor analysis study to estimate conditional core damage frequencies of critical LP&S events also revealed important findings related to human performance during LP&S conditions. First, it was determined that "operator response is probably the most important issue in determining the significance of an event in shutdown." The conditional core damage probabilities estimated for the events analyzed were "strongly influenced by the likelihood of failing to recover initially faulted systems over time periods of six to 24 hours."

Second, the analysts indicated that very little information existed concerning the ability of operators to implement the non-proceduralized short term actions which would be critical in the LP&S environment, thereby increasing the uncertainty of the calculated probabilities. When operator actions are non-proceduralized, the potential for misdiagnosis and errors of commission increased. These results emphasize the importance of adequate procedures for LP&S conditions and suggested that

at the time the events being studied occurred, emergency procedures may have been inadequate.

The results of the NRC site visits reiterated some of the findings discussed above in regards to non-proceduralized actions. It was found that although some plants provided in-depth preparation for actions related to critical needs like backup cooling, others placed more reliance on "ad hoc approaches."

In addition, the NRC teams noted that workers in several of the plants they visited felt pressured to reduce outage time further than the NRC team members judged to be prudent. Probably one of the most significant findings from the study was the wide variation in how the plants prepared for and conducted their outages. Other notable findings related to human performance included the following:

- In general, no plans were available for BWR containment closure or for dealing with conditions under which the containment may be challenged.

- Licensees acknowledged that Tech Specs did not fully address LP&S operations.

- Only one plant had an annunciator board that grouped major shutdown parameters.

Implication

Clearly, an important implication of the findings discussed in NUREG-1449 is that significant steps must be to taken to prevent and/or attenuate the impact of human errors during LP&S. Furthermore, it appears that the factors which influence human actions during LP&S (and their relative contributions to human errors) may be quite different than those in full-power modes. Given the wide variation in how the different plants handle LP&S conditions, a general and systematic approach for assessing human reliability in the LP&S environment is needed. The first step in the development of such an approach is to provide a systematic means for identifying where, what, when

and why human errors are likely to occur under LP&S conditions.

B.2.4.2.3 Evaluation of Shutdown and Low Power Risk Issues, SECY-91-283, September 9, 1991

SECY letter 91-283, issued on September 9, 1991, provides a status report on the staff's evaluation of safety risks that are unique to LP&S conditions and provides a revised action plan for completing the evaluation. The results of the ongoing staff activities discussed in the letter and in its Enclosures 1 & 2 have now been described in detail in NUREG-1449.

Enclosure 2 of the letter provided an action plan for addressing key issues related to LP&S conditions and for addressing some additional topics which warranted further evaluation. In describing the action plan, several points relevant to human reliability in LP&S conditions were made. The points are important and worth reiterating because they illustrate the uniqueness of the safety risks in the LP&S environment and support the need for the development of a specialized approach for identifying potential human errors and for assessing human reliability in such conditions. In addition, the points provide insights regarding the unique factors which are likely to influence human actions in LP&S conditions.

Outage Planning and Control

The report notes that during plant shutdown, maintenance and surveillance activities can result in the opening of the primary and/or containment systems, stoppage of the shutdown cooling system, disabling of electrical systems, and the movement of heavy equipment within the plant. Furthermore, many additional plant workers and contractors are actively involved; and because of the economic incentive to complete the outage expeditiously, many tasks are performed simultaneously. Although all plants have programs for planning and controlling outages, the degree to which risk management is included varies widely.

Stress on Personnel

Given the large amount of activity that takes place during an outage, the large work force involved, and the many and rapid changes in plant configurations and personnel assignments that can occur, the demands on plant personnel can be quite heavy. The excessive overtime that is often required to complete the outage on schedule can compound the problem and introduce stress that is unique to LP&S.

Need for Improved Training

Current operator licensing exams include little coverage of operations during shutdown. In addition, in simulator training there apparently is little coverage of activities during cold shutdown and refueling.

Need for Improved Procedures

The scope of the Abnormal Operating Procedures (AOPs) usually used for dealing with LP&S conditions is limited. These procedures lack adequate detail and symptom based procedures are not available.

Technical Specifications

The report concluded that current mode definitions in technical specifications were not detailed enough to identify risk significant conditions. Thus, inadequate guidance was provided to ensure plant safety.

Instrumentation for Shutdown Conditions

In some instances, inadequacies apparently exist in the instrumentation available for LP&S conditions. This situation can result in:

- Inability of operators to determine plant conditions;

- Reduced operator confidence in instruments;

- Inappropriate ranges;

- Critical indicators not being monitored.

Conclusion

The points listed above underscore the impact of the LP&S environment on human performance and reliability. Although many of the issues and conditions described can be resolved or improved through regulations and industry efforts, an adequate means of assessing the impact and influences of LP&S conditions on human reliability is needed. In particular, a method to evaluate the effect of design improvements on human reliability, and to evaluate the risk that remains after the improvements are implemented, is needed. Such a methodology will require a careful determination and analysis of the relevant human actions and the factors which influence those actions under LP&S conditions.

B.2.4.2.4   Residual Heat Removal Experience Review and Safety Analysis Boiling Water Reactors 1984-1989, NSAC/157, June 1991

NSAC/157 provides a review and analysis of Residual Heat Removal System (RHRS) operating experience and performance at Boiling Water Reactors from 1984 through 1989. The report extends a similar analysis conducted by NSAC which covered the period 1977 through 1983 [NSAC/88]. The review was initiated in response to industry awareness of unresolved generic safety issues associated with shutdown decay heat removal. It focused on plant events that occurred when the RHRS was operating in shutdown cooling mode during hot shutdown, cold shutdown, or refueling. Primary concern was with events that led to a loss or degradation of the RHRS, but some additional RHRS problems were also reviewed. The data base for the analysis came primarily from Licensee Event Reports (LERs), but event reports from the Institute of Nuclear Power Operations (INPO) and the NRC's Office for Analysis and Evaluation of Operational Data (AEOD) were also used.

In addition to summarizing RHRS operating experience, the goal of the analysis was "to identify areas where improvements in RHR performance can be made" and " to provide data about decay heat

removal systems for use in Probabilistic Risk Assessments (PRAs)." The analysis included evaluations of the role of human actions in the identified events, and the results and recommendations were relevant to human performance and reliability.

Principal Safety Concerns

The three principal safety concerns identified in the report included loss of coolant inventory, loss of decay heat removal system capability, and inadvertent pressurization.

According to NSAC/157, the more persistent problems occurring during LP&S conditions are related to losses or degradation of the RHRS due to loss of coolant inventory from the reactor vessel and losses of RHR due to inadvertent closure of RHRS suction valves. With regard to inadvertent pressurization, there have been BWR events during cold shutdown in which primary system pressure has increased above prescribed limits. The concern is that in the absence of operator or automatic isolation of the low pressure RHRS, damage to piping could occur. While no events of this nature occurred in U.S. plants during the period covered by NSAC/157, an event at an overseas plant occurred in which "operation of a high pressure control rod drive pump led to RHR isolation followed by inadvertent pressurization (1135 psig) of the reactor vessel and violation of vessel metal pressure/temperature requirements."

On the basis of NSAC/88, it appears that inadvertent pressurization events are generally related to hardware problems as opposed to human error. However, the importance of operator detection and response to such an event underscores the need for adequate operator training and properly designed instrumentation for LP&S conditions.

Loss of Coolant Inventory

Loss of coolant inventory events are a concern because there are a number of mechanisms for inventory loss in the RHRS that could result in uncovering the core. The potential for this event is

exacerbated by the fact that in some cases it can be initiated by a single mispositioned valve, and that during LP&S conditions not all of the protective features that can prevent core uncovery are required to be available.

NSAC/157 reviewed 17 loss of inventory events and six primary flowpaths were revealed:

- Unanticipated refilling of empty piping when placing the RHRS in shutdown cooling mode.

- Draining inventory to the suppression pool through misalignment of RHRS valves.

- Loss through minimum flow recirculation (pump bypass) line caused by inadvertently opening the min-flow valve to suppression pool.

- Suppression pool suction line valve is opened before the shutdown cooling line valve is closed.

- Draining the vessel to the suppression pool through inadvertent opening of automatic depressurization system valves.

- Draining to radwaste through RHRS discharge valves during lowering of suppression pool level.

All but one of the 17 identified events involved operator error or an inadequacy with the procedures being used. Five of the events occurred as a result of surveillance testing or component operability testing, and two others occurred in conjunction with maintenance activities. Most of the others were related to transferring RHR into or out of shutdown cooling mode.

Inadvertent Closure of RHRS Suction Valves

The most persistent problem identified (99 events) involved losses of the RHRS due to inadvertent closure of RHRS suction valves. The RHRS suction valves isolate automatically on containment

isolation signals from the reactor protection system. High reactor pressure, high flow high drywell pressure, and low reactor water level (Level 3) are conditions which will lead to valve closure. Of the 99 inadvertent suction valve closures identified in NSAC/157, 56 were determined to be caused by operational or procedural errors. Most of these involved simple human "slips" during maintenance or testing such as bumping cabinets or accidently shunting instrumentation with test equipment. Thirteen events resulted from inadequate procedures, with the rest apparently due to hardware failures.

Other Loss of RHRS Events

Additional loss of RHRS events reviewed in the NSAC/157 report were much less frequent than the types of events discussed above. They included:

-   Inability to establish RHRS flow due to inability to open RHRS suction valves;

-   Loss or degradation of RHRS due to other valve problems;

-   Loss of RHRS in conjunction with planned maintenance;

-   Loss of RHRS due to loss of the operating pump; and

-   Degraded RHRS cooling due to loss of heat sink.

Human errors related to these failures involved non-fulfillment of Tech Spec requirements, procedural inadequacies, and inadequate administrative controls.

Human Reliability Recommendations

The NSAC/157 report made a number of recommendations that were relevant to improving human reliability during LP&S conditions. Unique aspects of the shutdown environment and its impact on human performance were reflected in those recommendations.

First, the report indicated that improvements in management controls would reduce the frequency and severity of the types of events discussed. Recommendations included:

-   Improved personnel training regarding fuse pulling and valve alignment operations.

-   Plant investigation of relevant events and appropriate revisions in plant procedures.

-   Better coordination and management of contractor personnel who, due to unfamiliarity with the plant, inadvertently came in contact with breakers, circuit wiring, fuses, etc.

-   Updating manuals and drawings where installations and modifications have made them inaccurate and ensuring that the updated material is used.

Second, improvements in LP&S-specific procedures and practices were recommended as follows:

-   Improved procedures and practices for preventing and mitigating reactor vessel inventory losses.

-   Improved labeling (particularly for fuses and circuit breakers) and tagging of components and controls. Caution tags on control room switches which could lead to draining of the vessel. Audible alarms in the control room for closure of RHRS shutdown cooling suction line isolation valves. Information signs on motor control centers directing operators to applicable procedures for operating RHRS valves.

-   Prominent display and monitoring of key parameters important to decay heat removal (e.g., reactor level, reactor temperature, vessel pressure, and position of key power operated valves).

-   Improved procedures for starting and stopping RHRS pumps, for preventing water

hammer in pumps, and for preventing RHRS isolation valve closure. For the latter case, improved procedures to help prevent leads from being improperly lifted were recommended.

- Documentation of procedures which could be used to obtain alternate shutdown cooling methods.

Finally, improved testing and inspection of shutdown- related system components, more timely and thorough preventive maintenance, and plant modifications that respond to the demands of LP&S conditions, e.g., edge guards on rectifier fins to preclude grounding of circuits and better work space in panels and enclosures, were recommended.

The recommendations from NSAC/157 indicate that there are numerous human-system interactions which can lead to problems during LP&S conditions. It is apparent that administrative controls, training, procedures, task design, information display, and overall planning must be specifically tailored for the unique aspects of the LP&S environment. Moreover, any assessment of risk under LP&S conditions will have to consider apparent inadequacies in the support of human actions. This will require a careful analysis of the relevant tasks and factors which influence human performance and reliability during shutdown.

B.2.4.2.5 Guidelines for Industry Actions to Assess Shutdown Management, NUMARC 91-06, December 1991

The intent of this NUMARC document was to provide guidance to utilities on assessing and enhancing their current practices for planning and conducting outages. The underlying premise of this guidance was that proper management of outage activities could reduce both the likelihood and consequences of events that challenge plant safety during LP&S. The report notes that analyses of shutdown events have provided a better understanding of the vulnerabilities that certain systems and components have during shutdown

plant conditions and proceeds to provide guidance for addressing the vulnerabilities.

The major points and suggestions provided in the report include:

- The scope of activities that a utility undertakes during a normal refueling outage that make outage planning and control a significant challenge include:

  - refueling;
  - preventive and corrective maintenance;
  - modifications;
  - surveillance testing;
  - in service inspection; and
  - administrative activities that support the above tasks.

- Effective outage planning and control is the primary means of enhancing safety during shutdown. It requires:

  - a clear understanding of the utility safety philosophy;
  - appropriate involvement of organizational levels;
  - planning;
  - coordination;
  - communication;
  - an awareness of the plant status by personnel involved in the outage activities; and
  - thorough knowledge of which systems are available that provide and support key safety functions. (The key safety functions are: decay heat removal, inventory control, power availability, reactivity control, and containment).

- A senior management philosophy stating the utility outage nuclear safety philosophy should be established and communicated to personnel involved in the planning and execution of the outage.

- Outage schedules should be developed through interaction with involved organizations and

disciplines. The schedule should optimize safety system availability. Availability is defined as the system, component, or structure that is able to perform its intended service by immediate manual or automatic actuation. Outage activities should be controlled and implemented in accordance with the approved schedule. For any schedule change, the same philosophy and basis used to develop the initial schedule should be applied and criteria established that define the level of review and approval authority necessary to implement the change. A well-designed outage schedule realistically matches resources to activities. An outage overtime policy should be established. In addition, activities in the outage schedule should be sufficiently detailed and organized to accurately convey the shutdown risks due to the nature, grouping, or level of activities. Those activities that may impact key safety functions should be limited and strictly controlled. Outage planning and execution should consider the potential introduction of hazards such as fires and floods. The outage schedule should establish the systems, structures and components that will provide backup for key safety functions.

- The functionality (i.e., the ability of a system or component to perform its intended service even though technical specification requirements or licensing/design basis assumptions may not be maintained) should be assured by post maintenance testing, monitoring of key parameters with the system in service, or through verification of system alignment and administrative control by operations personnel. Systems, structures and components that provide backup of key safety functions or are necessary to optimize safety should be controlled. Procedures should be developed that are designed to mitigate the loss of key safety functions. The current status of the plant should be communicated on a regular basis to personnel who may affect plant safety.

- Contingency plans should be available when outage activities, plant configurations or conditions lead to the plant being more susceptible to a loss of a key safety function. Contingency plans are approved plans of activities that maintain safety by alternate means when pre-outage planning reveals that specified systems, structures or components will be unavailable. Personnel who may be required to implement the plans should be identified and familiar with them. The plans should consider the use of alternate equipment to respond to the loss of dedicated safety and monitoring equipment, and should also consider additional monitoring or controls to minimize the potential for unplanned equipment unavailability.

- A systematic approach to training on shutdown risks can enhance operator awareness and provide knowledge of the appropriate response to potential challenges. As much as possible, include simulator training for shutdown conditions in the training. Plant personnel, including contractors and others temporarily assigned to support the outage, should be trained in areas that are applicable to their particular role in the outage activities.

- Following development of the outage schedule and before final approval, a review of the schedule from a nuclear safety perspective will provide added assurance that the outage can be conducted in a safe manner.

- An extended loss of the decay heat removal (DHR) function can lead to boiling and potentially result in a depletion of reactor coolant and eventual uncovering of the core. The risk associated with a loss of DHR event is dependent on a number of factors, including the decay heat load present and the existing plant configuration. A comprehensive understanding of these factors is an essential element in effectively planning and controlling an outage and in effectively mitigating a loss of DHR event.

- Many of the events involving loss of DHR were initiated by outage activities (such as preventive maintenance and surveillance testing) on components within or that directly interface with

the DHR system. The planning and conduct of these activities is an important factor in reducing the likelihood of a loss of DHR event and the consequences of such an event.

- Many utilities have chosen to off-load the core to the spent fuel pool (SFP) during their refueling outages. This practice shifts decay heat removal requirements from the reactor coolant system (RCS) to the SFP. An event that results in the loss of SFP cooling may have the same undesirable effects as a loss of DHR event if appropriate compensatory actions are not taken.

- Control of the RCS inventory is essential to maintaining the overall DHR function. The reactor coolant system boundary expands during shutdown periods to include the decay heat removal piping, spent fuel pool, refueling canal and other connected support systems. This presents a significant number of potential inventory loss flow paths that are normally isolated during power operation. The RCS boundary is expanded because low-pressure systems, such as the DHR system, are connected to the RCS. The plant configurations and activities during outages increase the possibility of a valve misalignment that can result in a loss of RCS inventory. There are potential inventory loss paths through the DHR system to the suppression pool when DHR is aligned for shutdown cooling. Some can be initiated by a single mispositioned valve.

- Outage activities associated with the main steam lines such as safety/relief valve removal, automatic depressurization system testing and main steam isolation valve maintenance can create a drain down path for the reactor cavity and fuel pool. Some loss of fuel pool water events can result in draining the entire contents of the reactor cavity. In most plants, if the spent fuel pool were to be drained to the bottom of the fuel transfer canal or tube, the water level in the spent fuel pool would typically be below the suction piping for spent fuel cooling. Fuel being moved would be uncovered if the cavity drained.

Fuel with less than adequate water cover for shielding, including fuel being moved or suspended from manipulators, would result in high radiation levels in containment.

- Numerous events have occurred during shutdown as a result of the loss of AC power. This not only challenges the maintenance of key safety functions but also complicates recovery under abnormal conditions. AC power is required to: maintain cooling to the reactor core and spent fuel pool; to transfer decay heat to the heat sink; to achieve containment closure when needed; and to support other important functions. In the event that off-site and emergency AC power is unavailable, temporary hookups and the availability of alternate AC power can reduce risk. It is also necessary to maintain control over switchyard and transformer yard activities as this directly affects offsite power availability. Removal of AC and DC power sources from service or testing of these sources should not be performed when these sources are supporting systems that are actively providing key safety functions.

- There are two aspects of maintaining reactivity control: (1) maintaining adequate shutdown margin in the RCS and spent fuel pool; and (2) proper planning and control of all fuel handling activities. During periods of cold weather, the RCS water temperature can decrease below the minimum value used to analyze the reactor shutdown margin and the fuel pool shutdown margin. Cold water adds positive reactivity, decreasing the shutdown margin. During refueling, improper sequencing of control rods or fuel assemblies is possible because of numerous movements. For BWRs, soluble boron is not used to control reactivity during refueling, and therefore, reactivity margins are smaller than PWRs. Shutdown margins can be significantly reduced during refueling when control blades or fuel assemblies are not loaded in the proper sequence. Due to the limited number of source range monitors, the core reloading pattern is important. An improper loading sequence can allow regions of the core to approach criticality

without early detection by the source range monitor.

- During shutdown plant conditions, it is necessary to ensure that containment closure can be achieved in sufficient time to prevent potential fission product release. Containment closure is defined as the action to secure secondary containment and its associated structures, systems, and components as a barrier to fission product release under existing plant conditions. The time required for containment closure depends on a number of factors, including the decay heat level and the amount of RCS inventory available.

Several of the suggestions discussed in the NUMARC report were particularly relevant to improving human reliability and performance during LP&S. The suggestions include:

- clearly communicating management's philosophy and plan for ensuring outage safety to plant personnel;

- appropriately and systematically involving all plant organizational levels in the outage and its planning (i.e, maintaining integrated management);

- improving shutdown specific training for both plant personnel and contractors;

- improving shutdown specific procedures; and

- ensuring that plant operators have a thorough knowledge and awareness of which systems are available to provide key safety functions (e.g., decay heat removal, inventory control, power availability, reactivity control and containment) at all times during the outage.

These suggestions from the NUMARC report are in concurrence with the points relating to human reliability that were identified in the other reports reviewed. They clearly indicate that because of the unique plant conditions and circumstances that exist, a special set of requirements will be needed to ensure successful human performance during LP&S. The existence of these unique plant conditions and circumstances also indicates the need for an HRA methodology which will provide valid and reliable means for assessing their impact on human performance.

B.3 INTERVIEWS WITH KNOWLEDGEABLE INDIVIDUALS

B.3.1 Interview Protocol Development

B.3.1.1 Development of Interview Protocol for Utility Personnel

B.3.1.1.1 Purpose/Objectives

The purpose of the interviews with utility personnel was to obtain from operations/maintenance personnel their perspective regarding:

- The characteristics of LP&S operation that are significantly different from normal operation with regard to human performance and plant safety.

- The activities, operations, situations and human tasks that deserve attention in the development of a comprehensive HRA model for LP&S operations because of their potential safety implications.

- The characteristics and features of a good outage management program that should be considered in a model of human performance during LP&S operations.

- The processes used to identify safety significant events occurring during LP&S.

- Requirements and factors that influence performance of critical tasks.

B.3.1.1.2 Design

- Interviews were conducted using prepared questions and guidance for the interviewer, as it was necessary to assure a level of consistency and completeness and to maintain focus.

The interview guide was organized into three different sections, each with a different focus and using different approaches to obtain information. The complete guide is presented in Appendix E. The three parts were:

- Part I - Direct, open ended questions at a fairly high level to obtain input about important factors that differ between LP&S and normal operations with regard to human performance and safety, activities and human actions important to safety in LP&S, and important characteristics distinguishing safe performance during LP&S. Most questions were intended for all positions interviewed. Two questions (#6 and #7) were intended primarily for management level staff to identify characteristics of a good outage management program. Question 6 focused on "process" descriptions. Question 7 focused on "observable" performance indicators. Question 8 sought to identify important factors or challenges to safety by asking about barriers or preventive measures. Question 9 explored sensitivities to potential LP&S risk factors and human thought processes associated with assessing the importance and significance of LP&S occurrences.

- Part II - Questions of a more detailed nature, intended for supervisor level and below. The purpose was to focus on a small number of important human actions during LP&S and (through detailed questions) identify characteristics of human tasks as important contributors to human performance during LP&S, as well as specific kinds of human actions that may need to be modeled in a LP&S PRA. Question 14 solicits a subjective rating (low, medium, high) of the relative importance of eight factors potentially contributing to human performance. This question was typically asked in the context of human actions during LP&S in general, not with regard to a specific human action.

- Part III - A simplified "critical incident" approach in which the interviewee was asked to recall a specific plant situation which involved human errors (or particularly good human performance) and discuss it

using six questions as a guide. The purpose was to stimulate more in-depth discussion and specific examples from operational experiences which would elicit important information to be considered in the comprehensive HRA model. A critical incident approach is expected to be a comfortable format for operators to use to relate information through concrete "stories" rather than by responding to questions. This approach would be used as time permitted with experienced operations or maintenance personnel at the level of supervisor and below.

B.3.1.1.3 Interview Process for Utility Personnel Interviews

Eight individuals were interviewed in six separate interview sessions using the structured interview guide. Interviews typically lasted one to one and a half hours. Sections from the guide and individual questions from each section were selected in progress during the interview by the interviewees based on: time available; position and background descriptions of experience provided by the interviewee; and apparent areas of knowledge, experience or understanding of the interviewee. A separate half-hour interview was held with a group of individuals from the training organization immediately prior to closure of the two-day visit. That interview addressed several of the general issues that formed the basis for the structured guide, but did not follow the guide closely. A summary of the results from the utility personnel interviews is provided in Section B.3.3.1.

All interviewees were cooperative and open with their responses, though obviously there is an inherent interest in maintaining positive positions regarding Grand Gulf Nuclear Station (GGNS) operations and safety. The instructions from the interviewers and the nature of the questions themselves made it clear that focus of these interviews was collection of input and advice of a generic nature, not identification of strengths or weaknesses of GGNS. Consequently, there is no reason to suspect any significant impact on the responses due to a reluctance to discuss issues and

GGNS practice with outsiders, particularly NRC contractors.

B.3.1.2 Development of Interview Protocol for Non-utility Personnel

B.3.1.2.1 Purpose/Objectives

The purpose of the non-utility interviews was to capitalize on the substantial work already accomplished by NRC and industry organizations in collecting and assessing information on LP&S operations. All of the organizations/individuals selected have been key participants in previous studies, assessments or development of guidance related to safety in LP&S operations. These interviews were intended to focus on and summarize insights already gained from those assessments regarding human performance issues associated with LP&S operations.

B.3.1.2.2 Design

The interview subjects were a small sample selected to be representative of key senior individuals who had already participated in previous studies or NRC or industry actions regarding LP&S operations. A flexible interview guide with a small number of open-ended questions was desired to obtain insights, judgment and conclusions. Time available per person was expected to be approximately one hour. With these factors in mind, a six-question interview guide was developed. The first question was primarily for background on the individual's experience and recent focus on LP&S issues. It simply asks what particular aspects pertinent to human performance issues the interviewee has been addressing. Question 2 tries to identify specific studies, reports, guidelines, etc. that have been produced within the interviewee's organization. This assures completeness of our information sources and was of particular interest for organizations other than NRC. Questions 3 and 4 are the primary focus of the interviews. They ask directly the important lessons learned or insights from previous work and judgment on the most important characteristics of LP&S operation that impact safety. Questions 5 and 6 address the same

issues a little less directly by asking what factors distinguish good outage management performance from poor performance. This different perspective is intended to solicit information on key factors that may be important to include in the comprehensive HRA model by having the interviewee identify specific practices and factors that discriminate (and therefore influence) program quality and safety. A copy of the interview protocol used for non-utility personnel is presented in Appendix E.

B.3.1.2.3 Interview Process for Non-utility Interviews

All interviews were conducted in essentially the same manner. The interview began with one of the interviewers providing a brief overview of the purpose of both the LP&S HRA project and the interview itself. As a general rule, the discussions followed the order of the questions on the interview form and lasted between one and two hours. The results of the interview were consolidated by the interviewees from the notes taken during the discussion. The interviewees were very cooperative and informative.

B.3.2 Interviewee Experience

B.3.2.1 Utility Interviewee Experience

Utility interviewees included a fairly broad spectrum of plant personnel with direct experience in plant operations and maintenance, including operations under LP&S conditions. Seven Grand Gulf Nuclear Station (GGNS) were interviewed using the structured guide. They held the following positions:

- I&C Technician
- I&C Supervisor
- Surveillance Coordinator (formerly a Shift Supervisor)
- Operations Manager
- Outage Manager (formerly a Shift Supervisor)
- Emergency Planning/Procedures Coordinator
- HPES Coordinator (with previous operations experience)

In addition, an NRC Resident Inspector was interviewed using the guide. An abbreviated interview/discussion was held with a group of individuals from the training staff, including both operations and maintenance training and simulator instructors. Each of the seven GGNS staff identified above had multiple years experience at GGNS, and a number of them indicated that they had previous experience in other plants.

B.3.2.2 Non-Utility Interviewee Experience

A total of five interviews with non-utility personnel were conducted. The interviewees were involved in a diverse set of activities related to the study of safety issues in the low power and shutdown phase of operations. The NUMARC staff interviewed were members of the Working Group that produced NUMARC 91-06, Guide-lines for Industry Actions to Assess Shutdown Management. One NRC staff member interviewed with the Human Factors Assessment Branch, and primarily addressed issues related to procedures and training and the impact of stress on personnel. Another interviewee was an NRR human factors expert who had led or participated in several site visits related to low power and shutdown activities, including some visits as part of an incident investigating team (IIT). AEOD is responsible for reviewing operational events that could have generic impact. One of the AEOD staff interviewed was principally concerned with the human factor aspects of these events; the other was involved in the Accident Sequence Precursor Program. The EPRI staff member interviewed was from the Risk and Reliability Program in the Nuclear Power Division and responsible for their research program on low power and shutdown risk issues.

B.3.3 Results and Discussion of Interviews

B.3.3.1 Results and Discussion of Interviews With Utility Personnel (Grand Gulf Nuclear Station (GGNS) Operations Personnel, June 30 - July 1, 1992)

The results and discussion of the utility personnel interviews is presented by part and question of the interview guide.

B.3.3.1.1 PART I, Question 1 - Differences Between LP&S and Normal Operations:

- There are many more people on site and in the control room. At GGNS, the normal shift operating complement is essentially doubled by requiring personnel to work rotations of six, 12 hour days.

- There are more activities. Both the sheer number of activities and the physical pace of activities increase dramatically. This increase is accompanied by schedule pressure, workload stress, and greatly increased demands on communication and coordination.

- Increased work periods, especially long periods of overtime during LP&S, may increase the importance of fatigue as a detriment to human performance. However, GGNS interviewees did not think that the "six, 12s" are a problem for outages of 60 days or less.

- The nature of "procedural control" alters during LP&S operation. Work is still controlled by procedures, significant and safety-related operations, surveillances, etc. There are still have detailed procedures requiring strict compliance, and often require checkoff and/or signoff. However, LP&S operation is controlled more by work control procedures. In general, this means activities are more schedule-driven. Interviewees would not characterize LP&S operation as "less

rigidly controlled by procedure". However, there undoubtedly are differences between the nature of normal operating procedures and the nature of typical work control procedures. Also, it is clear that the level of "rigor" of operation during LP&S has increased over recent years.

- During an outage, plant configurations change dramatically and frequently. There are configurations that are quite different from normal operations and which are seen only during an outage. For a given outage, there may be rare or truly unique configurations. Further there are personnel from many different crafts, each with a different degree of plant knowledge, active during LP&S with whom the operator has to interact. These factors require an adjustment on the part of the operators and place greater demands on personnel in terms of awareness of plant status, communications, and knowledge of systems interactions and of the implications of human actions in a given plant state. In addition, personnel are less familiar with system responses during the non-routine configurations.

- The influx of contract personnel not thoroughly familiar with the plant and not fully integrated into the shift operation is a recognized issue. GGNS's practices to mitigate potential problems include a general policy to always have GGNS staff working with contractors and some site-specific training (though this training for contractors was not clearly identified).

- Tagging control was identified a number of times as a significant issue that is very important during an outage due to the greatly increased activities and the changing, non-routine configurations.

- Clearly, there is some LP&S-specific training for operators, maintenance personnel and technicians. It is obvious that much of "routine" training (e.g. - systems knowledge,

equipment operation, fundamentals) is applicable to LP&S as well as normal operations. However, it is also clear that training specifically for LP&S operations, especially training related to response to off normal events during LP&S operations, receives much less attention than for normal operations.

- It is recognized that significant changes in organizational responsibilities and management personnel may have a major influence on personnel performance and communications. All interviewees responding to this issue, however, indicated that this problem is minimal at GGNS because of specific administrative policies of keeping the same managers (all of whom have an operations background) in charge of all operations and key decision making. The outage management/control structure is superimposed on the normal operating structure. Key management positions in the outage structure are filled by the same managers who run the plant on a day-to-day basis. Supervisors are the regular supervisors who direct work during normal operations.

B.3.3.1.2   Part 1, Questions 2 & 3 - N/A

B.3.3.1.3   Part 1, Questions 4 & 5 - Challenges to Safety Functions

Activities, operations, or situations identified as potential challenges to safety were:

- Transition to DHR during shutdown.

- A stop/hold during shutdown or cooldown, or in attempting to control pressure.

- Any major system evolution or alignment (e.g., startup, valve lineup, flushing/warming).

- Any evolution involving moving water from/to reactor cavity for refueling.

- Installation or removal of main steam line plugs.

- Electrical bus maintenance/surveillance outage.

- Maintaining suppression pool level.

- Fuel movement.

- Shutdown cooling surveillance (I&C).

- Any vessel level calibration (I&C).

- Transferring from 60 to 15 cycle.

B.3.3.1.4   Part 1, Questions 6&7 - Good Outage Management Practice, Indicators of Good Outage Performance

Indications of good outage management practice and performance cited were:

- Clear identification of critical systems on a day-to-day basis throughout the outage. This includes identifying and physically marking equipment and areas critical to safety, training and daily briefings to make all personnel aware of the critical items and reminding them to not operate that equipment unless necessary and then not without taking special precautions.

- Supervisor performance, maintaining complete and constant awareness of the state of the plant and equipment and good communication to all personnel.

- Work control practice, ensuring rigorous, tight control over work in progress.

- Accurate work instructions, communicating good procedures that are readily available and rigorously followed.

- A good self-verification program. GGNS has a recognized program, now incorporated into their conduct of operations procedures, in which each employee is trained and

encouraged to perform a systematic "mental check" of each action taken, to assure that the action is correct and timely and that the system responds as expected.

- Maintaining good tagging practice.

- Checking that operators are knowledgeable and constantly aware of system and equipment status.

- Establishing good communications among all personnel.

- Managing good cooperation among various work groups and crafts.

- Checking for individual factors - alertness, constant awareness, knowledge.

B.3.3.1.5   Part 1, Question 8 - Measures to Mitigate Problems

At GGNS, typical "administrative controls" include:

- Procedures signoffs and checkoffs.

- Risk-based analysis of critical times and critical equipment during an outage, posting critical systems, and frequent (daily or more often) briefings to maintain awareness.

- Practice of using experienced operations people in management positions and keeping same people in charge during outage.

- Essentially doubling shift complement by using 6-12s rotation during an outage.

- Dedicated assignments for performing and coordinating critical and/or complex tasks.

- Dedicated days for work on specific divisions and working on only one channel at a time.

- Dedicated team of SRO and ROs for tagging control.

- Some LP&S-specific training.

- Outage schedule that drives and controls all activities.

- Self-verification program.

- Good labeling and color coding practice.

- Mixing plant personnel with contractors.

B.3.3.1.6   Part 1, Question 9 - Investigation of Events

Question was not sufficiently probed but, apparently, there is increasing emphasis on root cause analysis at GGNS.

B.3.3.1.7   Part II, Question 13 - Plausible Errors (two interviews)

Most questions in Part II were asked of three interviewees in two interviews. Some more detailed information was obtained from I&C staff on reactor pressure vessel level surveillance. The most significant input was gained from asking question 13 and question 14 from a general perspective (i.e., related to LP&S operations in general, not for a specific event). The results from question 13 regarding plausible errors were:

- I&C technician working on wrong equipment due to poor communication with control room.

- Electrician inadvertently taking wrong equipment out of service.

- Operators committing errors due to inattention or to tagging problems.

- Maintenance personnel inducing inadvertent actuations.

- I&C technicians causing inadvertent contact/short of leads; committing errors hooking up recorders for operators;

misplacing jumpers or incorrect lifting of leads; missing a step in a procedure.

B.3.3.1.8   Part II, Question 14 - Performance Influence Factors

There were four individuals in three separate interviews who responded to this question not related to a specific human action, but to human actions during LP&S in general. Their ratings (number of times selected) are shown in the table below:

IMPORTANCE TO PERFORMANCE
FACTOR

	LOW	MEDIUM	HIGH
Procedures		1	3
Training		3	1
Communications		1	3
Organizational factors	3	1	
Human engineering	1	1	2
Supervision	1	1	2
Stress	1		3
Engineering changes	1	3	

-    Procedures, communications and stress were considered to be of high importance to performance during outage; supervision and training medium-to-high. Human engineering received the most varied ratings, from low to high. Organizational factors had the lowest importance ratings and engineering changes were rated essentially of medium importance.

-    One interviewee provided responses specifically comparing the relative importance of the various factors for LP&S vs. normal operations. In comparison to normal operations, procedures, communications, human engineering, and supervision were felt to be of increased importance. Training and organizational factors were felt to be about the same importance in LP&S as in normal operations.

-    Individual comments recorded about the factors and reasons for ratings provide additional support for the ratings and additional insights into LP&S operations.

B.3.3.1.9   Part III

The information obtained from several interviewees regarding specific events that had occurred at GGNS tended to support, in general, the findings from the questions in the other section regarding typical kinds of operator errors and the major factors influencing human performance and human error. One interesting case is an error regarding the use of the wrong control rod drive tool which led to some problems during shutdown. It is not clear who authorized use of the tool, what analysis was done prior to its use, by whom, or what authorization was required. The underlying cause may be simply misjudgment or misoperation by an individual operator.   On the other hand, the incident may suggest a significant failure in management attention and control.

B.3.3.2   Results and Discussion of Interviews with Non-utility Personnel

Section B.3.3.2.1 summarizes the interviewees thoughts on what is unique about the LP&S activities and what are the important factors that influence human reliability in this phase of operations. Section B.3.3.2.2 summarizes what the interviewees felt to be the main lessons learned from their review of LP&S operations.

B.3.3.2.1   Unique Aspects of LP&S Activities That Impact Human Reliability

LP&S activities are characterized by frequent transitions in systems status and also by major transitions between plant operating modes. One interviewee felt that the particularly vulnerable phases are going into the outage with the change to a new working environment, and coming out of the outage where fatigue may be important. In addition, there are many more people on-site, many of whom are non-utility, contractor personnel. Site personnel may also be working under different conditions than

they typically do for normal full-power operations. For example, the practice may be to shift to 12 hour rather than 8 hour shifts, or the control room crew structure and responsibilities may be different. Another significant aspect of the low power and shutdown conditions that can impact safety is that the plant behavior is generally less well understood by the plant operators than is full power operations.

The protocol used in the interviews identified eight factors that have been proposed as influencing human performance, namely, procedures, training, communications, organizational factors, human engineering, supervision, stress, and engineering changes. While these factors may influence human performance in all phases of operations, certain aspects may be relatively more important in the LP&S phases, and the intent of the interviews was to identify these. These factors may also have a different influence on errors that lead to initiating events and errors during recovery from an initiating event. It was, however, difficult to draw conclusions directly from the responses to question 4b which addressed the relative importance of the factors as potential contributors to human performance. However, in the discussions generally, and particularly in the responses to questions 5 and 6 (see Appendix E), some useful insights were obtained and are discussed below.

The constantly changing plant status, and the increased activity in general, place increased emphasis on the need for efficient and timely communication of the changes taking place. In full power, activities are constrained and controlled by normal operating procedures and more stringent technical specifications. In addition, major plant modifications are generally made during shutdowns, and the non-familiarity with new equipment can impact plant personnel performance.

Those aspects of organizational factors and supervision that assure that lines of communication are established so everyone knows what to do and when to do it are also of increased importance in the LP&S phases due to the increased level of activity.

Establishing and maintaining defense-in-depth was felt to be important for preserving critical safety functions. This should involve careful control of maintenance activities to ensure that equipment required for performance of those critical safety functions is indeed available. Current Technical Specifications are felt to be generally inadequate in this regard. NUMARC has stressed that there should be procedures to deal with the loss of a critical safety function and contingency plans to restore defense-in-depth, should it be compromised. Absence of such procedures decreases the ability of the plant staff to respond to accidents should they occur and/or increases the chance of an initiating event occurring. The scheduling of work also has an influence on preserving defense-in-depth. For example, if functional tests on maintained equipment are delayed until plant start-up, this increases the exposure to any errors that may have been made in restoring the system.

Training the operators concerning the behavior of the plant during LP&S is important. For example, an appreciation of the time to boiling given loss of inventory, and knowing which instruments are reliable in what phase of operation are essential. Experience with operating in the LP&S condition is a positive factor; indeed, one of the contributing causes to the Prairie Island incident in 1992 was the lack of experience of the operators.

Human engineering may be an important factor which influences performance, but are there is probably no systematic impact induced specifically by LP&S conditions, as was the case with many of the other factors discussed above.

In summary, there are differences between LP&S and full power operations that arise because of the differences in the level of activity, the coverage and quality of procedures and other guidelines, the increased complexity of organizing work in the LP&S phase and the generally lower level of training in, and familiarity with, plant behavior. The opportunities for error are greater because of the increased level of activity.

B.3.3.2.2   Major Lessons Learned From A Review of LP&S Activities (According to Interviewees)

There was general agreement that one of the most important lessons learned from the study of LP&S operations is that good planning is essential to avoid or mitigate incidents that can impact safety. The plan should minimize the stress on personnel by scheduling work appropriately and also assure maintenance of defense in-depth with regard to critical safety functions. The plan should identify potential recovery actions and provide guidance to assure as much as possible that these actions be required, and their implementation is not hindered. This has been recognized more in recent years. For example, the containment hatch is usually now not sent off-site for work during refuelling as was the case for some plants in the past. Should it be desirable to close the containment quickly for those plants, it would not be possible to do so unless the hatch were at hand. Other examples were given where replacing the hatch was hindered by the presence of scaffolding in the opening, or in another case, where the electric motors required to move the hatch had been removed. In both cases, replacing the hatch cover would have been delayed, though not as dramatically as for the previous example.

One important feature of the plan should be establishing effective communications so that everyone has an up to-date view of the plant status, understands the philosophy of the outage, and understands which equipment has to be available. Each person must understand his role in the outage clearly. Procedures and guidelines must also be disseminated appropriately. The March 1991 event at Diablo Canyon occurred despite the existence of an in-plant procedure which was not adhered to.

Periods of major changes in plant status were felt to be the most vulnerable to the occurrence of initiating events. Therefore, effective communications during changes is a crucial factor.

One of the interviewees commented that, in some of the historical events, the timing was fortuitous and that if some failures had occurred somewhat earlier or later than they actually did, the consequences might have been different.

B.4 RESULTS AND CONCLUSIONS

The objective of this phase of the comprehensive human reliability analysis (HRA) project was to identify the unique characteristics, performance influencing factors, and error types which must be considered in selecting a methodology for HRA of low power and shutdown (LP&S) conditions. The conclusions developed from the results of the literature survey, events review, and interviews are presented in the following sections.

B.4.1 Classification of Human Actions

The classification of human actions and corresponding frequencies resulting from the LER review (presented in Section B.2.4.1) provide guidance for the kinds of human errors which should be examined and modeled in performing an HRA for LP&S. The data are particularly relevant for identifying and characterizing the nature of pre-accident human errors and for providing at least rough estimates concerning the contribution of human errors to important initiating event frequencies during LP&S. However, since less than 2% of the identified errors were identified as occurring during a response to an existing problem, the data are not generalizable to post-accident human actions. Conclusions from the classification results in regard to pre-accident errors, initiating-event related errors, and post-accident errors are discussed below.

B.4.1.1   Pre-accident Human Errors

The results of the LER review point out several areas in the pre-accident LP&S environment that should be carefully examined. Some of the more critical are noted:

- Clearly, Errors of Commission (EOCs) should be given greater attention than has been given in full-power PRAs. However, as noted in Section B.2.4.1, this should not be done at the expense of other types of human errors.

- Contractors/vendors accounted for 14.2% of the errors, and the kinds of tasks they perform

should be examined in performing an LP&S HRA. Guidance for this may be provided from further breakdowns of the LER data.

- Electrical-related components and activities were associated with a large number of errors and should be examined to determine which events have potentially dangerous consequences.

- In general, procedures were identified as being one of the most critical performance influencing factors. This implies that "adequacy of procedures" will be an important factor in assessing a given plant's risk during LP&S.

- For loss of shutdown cooling events, supervision was identified as an influencing factor 40% of the time. This result suggests that supervision is also an important factor to consider in assessing shutdown risk, at least for some classes of events.

B.4.1.2   Initiating Event Frequencies

Several initiating event frequencies approximated from the LER data clearly indicate the importance of carefully examining the human contribution to such events. The frequencies included:

- Loss of SDC: 0.98 events/calendar year, 3.28 events/shutdown year

- Loss of reactor coolant inventory: 0.24 events/calendar year, 0.82 events/shutdown year

- Loss of electrical power: 0.57 events/calendar year, 1.91 event/shutdown year

- Inadvertent ESF actuation: 2.47 events/calendar year, 8.25 events/shutdown year

Given the potential challenges to plant integrity that could arise from such events, the factors which influence human error should be evaluated and their impact addressed in assessing plant risk.

B.4.1.3 Post-accident Human Errors

While the results of the LER data provide some insights regarding factors relevant to operations in the pre-accident LP&S environment, whether or not those insights are relevant in the post-accident context remains to be determined. As has been indicated throughout this report, LP&S-specific conditions and factors clearly influence the operators' ability to respond to an initiating event. These performance influencing factors will need to be examined in the context of the operators' decision processes which occur in response to the accident scenario. Obviously, the role of plant procedures will be critical in such situations and their influence on operator decision processes should be modeled explicitly in the PRA context.

B.4.2 Influences on Human Reliability

The literature review, event review, and interviews identified several factors which influence human reliability during LP&S. The identified performance influencing factors are described below.

B.4.2.1 Administrative Controls

In this context, the term "administrative controls" refers to procedures and practices a plant uses to define and implement safety criteria for LP&S operation. These would include formal administrative procedures (e.g., Conduct of Operations - Outage), shift orders, outage planning guidelines, or informal practices observed by a significant portion of the staff.

Administrative controls are particularly important to human reliability during LP&S when Technical Specification coverage is limited. Controls which clearly specify and effectively implement comprehensive safety criteria will limit the likelihood of human error.

B.4.2.2 Human Factors Engineering

This performance influencing factor refers to those aspects of the environment and man-machine interface which affect human performance. Significant human factors issues identified in the study include:

- Accessibility of leads and jumpers inside instrument cabinets
- Component labeling
- Color coding by functional train
- Communication media and procedures

B.4.2.3 Operator Training

The level of operator training in LP&S operations varies considerably and is believed to be a critical factor in the reliability of operator actions during off-normal events. Classroom training on LP&S conditions, as well as simulator training, are important factors.

B.4.2.4 Workload and Stress

In the context of nuclear power plant operations, these factors are often closely related and can be considered together. Increased workload and stress were cited often in the literature as contributors to human error during LP&S. However, the GGNS plant staff interviews indicated that high workload and stress, while potentially significant, did not appear to be at detrimental levels at the plant.

During the outage at Grand Gulf, the size of the operations crew is expanded and the shift organization is changed to minimize the impact of the increased workload and reduce the stress of outage operations. These measures were cited by the staff as effective in minimizing the impact of outage operations on workload and stress. It may be that staffing and organization can be used as influencing factors rather than the more difficult to measure factors of workload and stress.

B.4.2.5 Procedures

The format and coverage of abnormal operating procedures are important factors affecting human error in recovery actions. Procedures for surveillance, maintenance, or special evolutions are an important factor in human error initiated events.

B.4.2.6 Awareness

Because of the critical role of the operator in LP&S operations and the increased susceptibility to events initiated by non-operations personnel, the level of awareness of current plant configuration and vulnerabilities is an important factor influencing human reliability. Measures such as shift briefings, warning signs, status boards, and caution tags are used to promote awareness.

B.4.2.7 Verification

Measures to verify correct performance of difficult or critical tasks are another important influencing factor. Many plants require second person verification for critical system lineups or evolutions. Several plants have recently implemented procedures for self verification on routine tasks.

B.4.3 Differences in Influences and Actions at LP&S vs. At Power

The literature review and interviews identified a variety of factors which are unique to LP&S operation as compared to operation at power. Many of these factors may limit the applicability of HRA methods traditionally used in PRA studies of full power operations. The LP&S conditions which were found to have the most significant impact on the selection of an HRA methodology are described below.

B.4.3.1 Human Error Initiated Events

The most significant difference between full-power and LP&S operations is the number of opportunities for human error to initiate a challenge to a critical plant safety function. This difference was cited several times in the literature and by most of the experts interviewed. The incidence of human error initiated events was also evident in the LER data.

A typical outage will involve thousands of operational configuration changes, maintenance tasks, and special evolutions. These activities are performed over a relatively short period of time and human error can result in interruption of decay heat removal, loss of reactor coolant systems (RCS) inventory, or uncontrolled criticality.

During power operation the frequency of interactions with critical systems and the potential for functional failure resulting from human error are much lower.

Many of the maintenance tasks and special evolutions performed during an outage are prohibited by technical specifications or procedures during plant operation at power.

B.4.3.2 Less Explicit Safety Criteria

The criteria defining safe operation, such as allowed system configurations, equipment operability, or control room staffing are less explicit for LP&S than for power operations. Technical Specifications (TSs) provide specific safety criteria and are rigorously adhered to in all aspects of plant operation. However, as frequently stated in the literature and the interviews, TS coverage in LP&S is far less comprehensive than coverage of power operations. In many cases TSs do not provide assurance of safe LP&S operation and there is little correspondence between TS compliance and safety.

To supplement the requirements of TSs during LP&S, many plants have developed additional safety criteria which are implemented through administrative procedures, policies, or practices. However, these criteria are often not as well understood or adhered to as TSs and can be changed with far less review and approval.

B.4.3.3   Incomplete Procedures Coverage

Emergency Operating Procedures (EOPs) for power operations have been developed over many years and in compliance with stringent regulatory requirements. The "symptom-based" EOPs have been structured to minimize diagnostic requirements on the operators and to explicitly state all critical operator actions. These procedures are continuously verified and updated based on industry experience and training exercises.

In contrast, the abnormal operating procedures (AOPs) covering LP&S events typically do not provide comprehensive coverage. The NRC specified criteria that apply to EOPs, such as writing guide and verification documentation do not apply. For this reason, AOPs often do not receive the same level of review and quality control as EOPs and may be inconsistent in format and content.

Although there have been recent efforts to expand the coverage of LP&S operating procedures, the wide variety of plant conditions possible in LP&S makes detailed coverage of all likely situations difficult. The literature and interviews identified many situations where no applicable procedures existed.

B.4.3.4 Dependence on Human Interactions

LP&S operation is more operator intensive than power operation. Equipment configurations change frequently, few automated responses occur and there is less equipment redundancy. For these reasons, there is a much higher dependence on operator actions during normal and off-normal conditions. Thus, the likelihood of operator error is higher during LP&S operation than during power operation.

B.4.3.5   Operator Response Time During Abnormal Events

For most of the abnormal event sequences identified in the LP&S PRAs and LER data review, the time available for operator response is considerably longer than for power operations. The course screening analysis of Grand Gulf indicated that 2.2 percent of the high Core Damage Frequency sequences could be terminated by appropriate operator action within 14 or more hours. Many of the remaining high CDF sequences had at least two hours for recovery.
In contrast, critical operator actions during event sequences at power must be performed within a much shorter time span.

B.4.3.6   Variation in LP&S Operation

An important conclusion drawn from the literature review and expert interviews is that there is large variation in the characteristics of LP&S operation which affect human reliability. As noted above, the regulatory requirements applicable to LP&S operations are much less prescriptive than for power operation. Plants have considerable latitude in the implementation of safety criteria and controls. Differences in safety philosophy, utility resources, and plant design result in significant differences in the conduct of LP&S operations between plants.

An equally important source of variation is the recent emphasis on LP&S operations throughout the industry. The NRC, NUMARC, INPO and EPRI each have significant programs underway to support improvements in LP&S operation. Most plants have recognized the risks of LP&S operations and are in the process of implementing changes. This broad-based movement to improve the conduct of LP&S operations makes it difficult to characterize existing practices and identify effective measures.

B.5 REQUIREMENTS AND RECOMMENDATIONS FOR COMPREHENSIVE HRA

Requirements for the LP&S comprehensive HRA methodology and recommendations for additional research are presented below.

B.5.1 Requirements

The conclusions discussed in Section 4 indicate that the HRA methodology to be used for LP&S will have somewhat different requirements than the methods often used in PRA of full power events. These different requirements are summarized as follows:

B.5.1.1 Errors of Commission

Errors of commission will likely be an important part of HRA for LP&S sequences. This is because of the increased opportunity for human error initiated events and the generally less specific safety criteria. In full power PRA, commission errors are typically not explicitly modeled. An improved HRA method will have to determine the extent to which EOCs should be modeled.

B.5.1.2 Time Response

In full power PRAs, one of the major HRA areas addressed is operator response to transients and major events using abnormal/emergency operating procedures. These actions are usually time-critical, and typical HRA models have stressed time available vs. time required as a major determinant of estimated operator reliability, (e.g., time reliability correlations). In LP&S operations there will be some procedure-driven, time-critical responses to initiating events that can be treated using existing models. In many cases, however, the time available for action (and for detection and correction of errors) is long compared to the time required to perform the action. The human performance involved is simply not time-critical. Thus, existing time reliability correlations will not be applicable and a different approach will be required.

B.5.1.3 Diagnostic and Knowledge Based Tasks

The variety of plant configurations and frequently incomplete coverage of procedures in the LP&S condition results in much greater reliance on operator diagnostic skills and plant knowledge in recovering from initiating events. Existing models for such "cognitive" behavior that have been used in full power PRAs are extremely simplified. In some cases, analysts have made the assertion that because operator response is tightly specified and controlled by EOPs, there is very little diagnostic or knowledge based behavior involved. It is difficult to justify taking credit for non-proceduralized actions, and often they are simply ignored. For HRA in LP&S operation it will be necessary to address these kinds of tasks, and improvements to existing models will be required.

B.5.1.4 Variation in Conditions and Influencing Factors

Full power operations are fairly standardized when compared to the wide variation in conditions and influencing factors encountered in LP&S. Therefore, the HRA methodology will have to be highly robust to account for the full range of situational and influencing factors affecting LP&S task performance.

B.5.1.5 Applicability of HRA Data

Most of the Human Error Probabilities (HEPs) currently used in the HRA portion of full power PRAs are developed from analysis of full power operations. To some extent, the HEPs are anchored to experiences from simulator exercises. These estimates will not, in general, be applicable to tasks performed under LP&S conditions. The HRA methodology will require some approach for validating the estimates as being applicable to LP&S situations. It should also be noted that estimates developed from nuclear plant experience in LP&S operations may not be accurate for current or future situations. The practices for the conduct of outages have changed considerably in the past year and are

Requirements

expected to continue to evolve over the next several years. Thus, data from plant experience may have to be adjusted to account for these changes.

B.5.2 Recommendations

The requirements discussed above suggest the need for development of an HRA methodology applicable to LP&S conditions. However, one or more of the existing HRA methods may be adaptable to the LP&S environment, if appropriate data on LP&S human error probabilities and influencing factors can be obtained.

It is recommended that a systematic review of current HRA methods used in nuclear plant PRA and other applications be conducted to assess these methods against the requirements described above. The results of this study should be used to prepare a "requirements specification" for an HRA methodology for PRA of LP&S operation. The methodologies to be reviewed should include those developed for nuclear plant PRA (e.s., THERP, ASEP HRAP, SLIM/MAUD, EPRI) as well as those used in similar applications (e.g., MANPRINT-DOD). The results of this review would be an assessment of where additional methodology development and adaptation are required.

Once the above is accomplished, research should be conducted to develop methods and criteria to evaluate and quantify the effects of LP&S situational and influencing factors on human performance. Because of the large variation in these factors, a systematic and practical process of accounting for the plant specific conditions in determining human error frequencies and probabilities is essential to any HRA of LP&S operations.

A final recommendation concerns the development of human reliability data for LP&S conditions. Of primary importance are data on the frequency of human errors resulting in initiating events. These human error frequency data should be derived from a detailed analysis of shutdown operating experience. Data on diagnostic and knowledge based recovery tasks may be developed from simulator exercises of shutdown events.

APPENDIX C

HUMAN RELIABILITY INFLUENCES

DURING LOW POWER AND SHUTDOWN CONDITIONS

IN PWR NUCLEAR POWER PLANTS

W.J. Luckas,[1] J. Wreathall,[2] S.E. Cooper,[3] M.T. Barriere,[1] and W.S. Brown[1]

[1]Brookhaven National Laboratory
Department of Nuclear Energy
Upton, NY

[2]John Wreathall & Co.
Dublin, OH

[3]Science Applications International Corp.
McLean, VA

Table of Contents

Table of Contents (continued)

Tables

*   Source - AIT Report.
** Source - AEOD Human Factors Report.

Abbreviations

AEOD	NRC Office for Analysis and Evaluation of Operational Data
AIT	Augmented Inspection Team
AOP	Abnormal Operating Procedures
BWR	Boiling Water Reactor
CCW	Component Cooling Water
CR	Control Room
CVCS	Chemical Volume and Control System
CRO	Control Room Operators
EDG	Emergency Diesel Generator
EOP	Emergency Operating Procedure
EPRI	Electric Power Research Institute
ES	Engineered Safeguards
ESFAS	Engineered Safety Features Actuation System
ESW	Emergency Service Water
HACS	Human Action Classification Scheme
HPIP	Human Performance Investigation Process
HRA	Human Reliability Analysis (or Assessment)
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
IAE	Instrumentation and Electronics
IIT	Incident Investigation Team
INPO	Institute of Nuclear Power Operations
LER	Licensee Event Report
LOCA	Loss of Coolant Accident
LP&S	Low Power and Shutdown
LPI	Low Pressure Injection
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission (or U.S. NRC)
NUCLARR	Nuclear Computerized Library for Assessing Reactor Reliability
NUMARC	Nuclear Utility Management and Resources Council
NSAC	Nuclear Safety Analysis Center
NSO	Nuclear Station Operator
POS	Plant Operational State
PRA	Probabilistic Risk Assessment
PWR	Pressurized Water Reactor
PZR	Pressurizer
RAT	Reserve Auxiliary Transformer
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RO	Reactor Operator
RV	Reactor Vessel
SCRE	Shift Control Room Engineer
SCSS	Sequence Coding and Search Scheme (for LERs)
SDC	Shutdown Cooling
SE	Shift Engineer

C.1 Introduction

C.1.1 Background

During Low Power and Shutdown (LP&S) conditions in a nuclear power plant (NPP), there are more direct human interactions with the unit's systems (via such activities as operating, maintaining, testing, reconfiguring, etc.) than during power operation conditions. Therefore, an assessment of LP&S related risk needs to include a greater emphasis on human reliability than such an assessment made for power operation conditions. As used here, LP&S conditions are met when a NPP reactor is subcritical (shutdown) or at less than 10-15% power.

When a NPP enters LP&S conditions, its normal power operation configuration is altered substantially such that there is less automated control. As a result, control of the unit during LP&S conditions is maintained almost entirely by human interaction through manual control rather than automated control. Also, during low power and especially during shutdown, there is generally much less equipment available for use. This increased unavailability of potential backup equipment is due to increased activities of maintenance, testing and modification. Thus, during LP&S, the human interactions with the unit systems will be more frequent and direct with considerably less backup by either manually or automatically activated equipment.

In order to properly account for the increase in human interaction and thus be able to perform a probabilistic risk assessment (PRA) applicable to operations during LP&S, it is important that a comprehensive human reliability assessment (HRA) methodology be developed and integrated into the LP&S PRA. In this manner, the PRA will more accurately incorporate the many reported human actions (both errors and recoveries) which may prove to be important during LP&S conditions and quantify their associated human reliabilities using the appropriate reliability influences. With such a comprehensive HRA as a key ingredient of an integrated LP&S PRA/HRA, the resulting risk assessment would provide a more realistic and justifiable model of a NPP at shutdown or low power conditions.

The tasks comprising the comprehensive HRA methodology development are as follows: (1) identification of the human reliability related influences and associated human actions during LP&S, (2) identification of potentially important LP&S related human actions and appropriate HRA framework and quantification methods, and (3) incorporation and coordination of methodology development with other integrated PRA/HRA efforts. Only after these tasks are completed will the PRA/HRA detailed quantification be performed.

An assessment of human reliability influences and any associated human actions during LP&S conditions for a U.S. NRC licensed pressurized water reactor (PWR), namely the results of the first task mentioned above, is the subject of this Appendix C.

C.1.2 Objectives

The objectives of this appendix are as follows: 1) to identify classes of human actions (errors and recoveries) during LP&S conditions, (2) to identify LP&S related human reliability influences (also referred to as human performance shaping factors) and assess their relative contribution to human error, (3) to assess the differences between human reliability influences and any associated human actions during LP&S conditions and those modeled in full-power PRAs and (4) to propose human reliability influences to be incorporated into the integrated PRA/HRA detailed quantification for LP&S conditions.

C.1.3 Approach

The assessment of human reliability influences and associated human actions during LP&S conditions consisted of two essentially sequential phases. First, a review of appropriate reports and reported

events was conducted and a classification of selected human actions was developed; second, based on the review results and previous experience, an interview protocol was developed and interviews were conducted with knowledgeable personnel from NRC, industry, and a NPP.

C.1.4 Terminology

Table C.1 provides the terminology used in both the assessment of human reliability influences and associated actions for LP&S and this report describing the results of this assessment.

C.2 Review of Reported Events and Associated Studies and Classification of Event-Specific Data

C.2.1   Introduction

The major effort in identifying and classifying human actions and influences impacting human performance during LP&S conditions consisted of gathering and evaluating appropriate sources of data. Various data, both event-based and non-event-based, were collected. A classification scheme was developed and applied to the evaluation of event-based data. These evaluations yielded various insights with respect to the occurrence of human errors and recovery actions and their associated influences during LP&S.

C.2.2   Classification Scheme Development

The Human Action Classification Scheme (HACS) was developed in order to organize information important to human performance from event data for LP&S conditions. The development of this classification scheme was influenced by the important issues identified in reports related to LP&S conditions, experience in evaluating event data for human performance issues, the intention to store the collected information in a computer data-base, and the process of applying the scheme to the specific event data evaluated for this project. The rationale for the various fields included in HACS and the origin of certain features of HACS are discussed briefly below.

C.2.2.1 HACS Information Fields

The event information collected is intended to serve four major purposes. First, each event is uniquely identified by the plant involved, the date of occurrence, and the impact of the event upon the plant (e.g., loss of shutdown cooling, loss of offsite power). Second, the plant configuration and available equipment at the time of each event is identified as pertinent to the initiation of the event and mitigation options. Third, based upon actual or potential consequences, each event's severity is assessed. Finally, but most importantly to this project, human performance information is gathered in order to identify human reliability influences (i.e., performance shaping factors) and associated human actions (i.e., initiators, latent errors, or recovery actions). The specific information collected and corresponding HACS fields are:

Event information. (Fields 1-3) Information uniquely identifying each event includes: the document number (including plant docket number), a brief event description, and the time of occurrence (i.e., date and time).

Plant state and conditions. (Fields 4-7,23) The plant type and vendor, the status of the plant (i.e., Plant Operational States (POSs)), note-worthy plant conditions (i.e., plant configuration, equipment out of service, etc.), and the status of other units at the time of the event is noted. In addition, the automatic response of equipment as it pertains to effective event mitigation is recorded.

Event severity. (Fields 24-27) The severity of the event is estimated by noting, when report-ed, the fission product barriers breached and other radiological effects. Also, an assessment is made with respect to the uniqueness of the event to LP&S conditions and the general level of risk significance.

Human action information. (Fields 8-22,28) Collection of a variety of human action information is accommodated by HACS. All human actions (latent, initiating event, and recovery) are identified and briefly described. For each human action, information typically pertinent to human reliability analyses can be documented within HACS, as applicable:

Table C.1.
Terminology Used for Assessment of Human Reliability Influences

Human errors: The terms "human error" and "unsafe act" are used interchangeably. The term human "error" is taken to be an action that is judged to have been inappropriate in the circumstance (see, for example, Senders and Moray in Section 5). As observed by Reason (again, see Section 5), these unsafe acts are those actions (or lack of actions) by people that are the operators and maintainers of equipment, that cause a potentially dangerous condition. In well-protected systems, defenses exist to prevent these unsafe acts from becoming incidents and accidents. These defenses can include hardware (e.g., safety systems, interlocks) and administrative controls (e.g., procedures, rules of conduct).

Classes: Different classes of human errors and actions are modeled in PRAs, namely:

Initiator: A human initiator is an (active) human action which starts an accident or incident.

Pre-accident: A pre-accident human error (latent) is an error which occurs prior to an abnormal event and which is discovered during an accident or incident.

Recovery: A recovery action is an (active) human action taken in response to an abnormal event in order to mitigate the consequences of the accident or incident.

Post-accident: A post-accident human error is an active human error which occurs in the response to the accident (i.e., a failed recovery action).

Error effect: With respect to the effect upon the plant, errors or unsafe acts can be either active or latent.

Active: The consequences of these errors are immediately revealed (e.g., initiator).

Latent: The consequences of these errors lay dormant in the plant until triggered by some event (e.g., deficiencies in maintenance, improper valve lineup).

Error mode: Errors or unsafe acts are committed in one of two modes, e.g.,

Omission: Errors of omission are failures to perform actions to maintain plant defenses (e.g., failing to start emergency equipment). Sub-categories: 1) omission of task, analysis, or step; 2) omission within allotted time; 3) omission of alarm response; 4) omission of adjustment or calibration; 5) other omission human factor.

Commission: Errors of commission are actions that cause (i.e., initiate) or exacerbate an abnormal event. Sub-categories: 1) commission of undesired task, analysis, or step; 2) commission of undesired alarm response; 3) commission of undesired calibration or adjustment; 4) other commission human factor.

Error type: Errors are differentiated by type with respect to the involvement of cognitive processes, i.e.,

Slip: Slips and lapses are unsafe acts where what was performed was not what was intended. Sub-categories: 1) correct intention, action not executed as planned; 2) inadvertent actuation or disabling of equipment; 3) selection of wrong item or failure to follow procedure.

Mistake: Mistakes are failures where the intentions are erroneous, but are purposefully executed (e.g., a misdiagnosed failure in a component resulting in a repair which is irrelevant to the failure mode). Sub-categories: 1) planning inadequate, although action went as planned; 2) faulty diagnosis of problem; 3) incorrect procedure used; 4) procedure not used; 5) miscommunication.

Table C.1.
Terminology Used for Assessment of Human Reliability Influences (continued)

Error type:	(continued)
	Circumvention: Circumventions are deliberate but non-malicious violations of safety rules often done for "good" reasons such as overcoming some organizational barrier. Sub-categories: 1) forced - conflicting demands for action results in an action deliberately not performed; 2) planned - action taken which deliberately does not follow routine; 3) actions taken to gain an advantage in time or in performing testing too quickly to finish early, or performing two tests simultaneously; 4) re-prioritized - priority of activities caused deferment of testing or surveillance.
Event significance:	The significance of the LP&S events which were evaluated for the HACS data base were also assessed and categorized with respect to their safety significance. The three different categories which were used are:
	Major: A major event is one whose importance is assessed to be relatively high.
	Minor: A minor event is one whose importance is assessed to be relatively low.
	Detectable: A detectable event is one whose importance is assessed to be relatively insignificant.
Influences:	Influences, or performance shaping factors, are those factors which affect human performance and reliability (e.g., procedures, training, communication).
Influence attributes:	Attributes of influences are those specific positive or negative aspects of influences (e.g., procedures: steps inapplicable to shutdown) which can impact human reliability and which can be audited in a human reliability assessment for the purposes of quantifying human error probabilities.

personnel type (e.g., control room (licensed) operator); activities being performed (e.g., maintenance, testing, operations); location of action (i.e., in-control room or ex-control room); error mode (i.e., omission or commission); error type (i.e., slips, mistakes, or circumventions); active or latent errors, and influences (e.g., procedures, communication, human engineering) on human performance. HACS also accommodates documentation of long-term corrective actions indicated in the event data which are pertinent to the human actions identified. Other information accommodated includes the system(s) involved and the human action descriptor (e.g., start pump, isolate leak).

C.2.2.2 Origin of HACS Information Fields

HACS has its origins in several existing coding schemes which have been combined. However, the original coding schemes have been modified to meet the event data evaluation needs of this project. In general, the modifications consisted of additions to the original coding scheme in order to capture information considered important and relevant to human actions during LP&S conditions and factors influencing their performance. Specific HACS fields which have been adapted from existing coding schemes are:

Event Description Summary. (Field 2)
Standard phrases describing each event are used in HACS to facilitate database sorts by event type. The types of events identified in draft NUREG-1449 were used as the basis for this field's coding scheme.

Unit Status. (Field 5) The PWR Plant Operational States (POSs) developed for use in the Level 1 PRA effort are used for this field.

Other Unit Status (Field 7), Personnel Type (Field 9), Event Activity (Field 10), Acts of Human Error Omission and Commission (Field 16). The documentation in these fields is based upon the coding scheme used for LER Sequence Coding and Search Scheme (SCSS) summaries.

System Identification. (Field 12) The source for the system codes used in HACS is IEEE STD 805 - 1984, Recommended Practice for System Identification in Nuclear Power Plant and Related Facilities. This coding scheme is increasingly used also in "full-text" LERs.

Component Identification (Field 13), Display/Instruments/etc (Field 14), Human Action Descriptor (Field 15). The Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR) (NUREG/CR-4639, Volume 4) is the basis for these fields.

Error Influences. (Field 19) Many classification schemes exist for the characterization of human errors. This project adopted the classification of influences impacting human performance used in the Human Performance Investigation Process (HPIP) (NUREG/CR-5455).

Uniquely specified fields in HACS include: the event time, noteworthy plant conditions, the human action location, specification of an active or latent human error, recovery time, recovery location, recovery origin, the automatic response of equipment relevant to event mitigation, the assessed level of risk significance, the uniqueness of the event to LP&S conditions and corrective actions taken.

C.2.3 Sources of Information Reviewed and Evaluation of HACS

The sources of data available to identify human actions and influences impacting human performance are divided into two groups; those that provide direct, actual event-related human action data, and those that also provide human reliability information, but not from a specific event. The data source documents are identified in Section C.5, References.

C.2.3.1 Event Data Sources

The actual event-related human action data are derived primarily from documents providing the most level of detail about the particular event with a minimum of previous analysis. Three principal sources of data were used. These were (1) NRC Augmented Inspection Team (AIT) reports, describing significant LP&S events, (2) NRC AEOD reports describing significant human factors LP&S events, and (3) full-text LP&S Licensee Event Reports (LERs). The human action data derived from AIT and LER sources are categorized in accordance with HACS, and along with the AEOD source, include only plant-specific events. The preferred data source was the AIT reports because of their detailed and independent evaluations of the circumstances of these significant events. Due to the small number of such evaluations, selected full-text LERs were also reviewed. Table C.2 shows the data sources for event-based data which formed the major portion of the evaluations.

Since there are literally thousands of LP&S-related LERs for PWRs mentioning human performance issues, the strategy used for LER sampling was to concentrate on events referenced in draft NUREG-1449. In particular, those PWR LP&S events which have been included in the evaluation were those used as part of the NRC AEOD Special Evaluation Report on shutdown and refueling and the NRC Accident Sequence Precursor methods, as noted in draft NUREG-1449.

Using the March 1990 Vogtle Unit 1 event as an example, Table C.3 illustrates the typical amount of information detail found in summary LERs, full-text LERs, and event-based reports. In general, the most important information to the objectives of this endeavor consist of pre-existing plant conditions; the number, type, and other characteristics of human errors (and actions); and influences on human errors

Table C.2.
Sources of Event-Based LP&S Data

| Plant | Data Sources | |
	LERs[1]	NRC Reports
ANO-1	10/26/88 12/19/88 12/05/89	
ANO-2	05/04/88	
Braidwood 1	12/01/89	12/01/89 - AIT Report. 10/04/90 - AEOD Human Factors Study Report.
Braidwood 2	02/23/89	
Byron 1	09/19/88	
Catawba 1	04/28/85 04/22/85	03/20/90 - AEOD Human Factors Team Report.
Crystal River 3	02/02/86 10/16/87	12/08/91 - AEOD Human Performance Study Report.
Diablo Canyon 1		03/07/91 - AIT Report.
Diablo Canyon 2	04/10/87	04/10/87 - NUREG-1269.
Farley 2	11/27/87	
Fort Calhoun	03/21/87 02/26/90	
Haddam Neck	08/21/84	
Harris 1	10/11/87	
Indian Point 2	11/05/87	
McGuire 1	09/16/87 11/23/88	
Millstone 2	12/09/81 02/04/88	
Oconee 3	09/11/88	03/08/91 - AIT and AEOD Human Factors Study Reports.
Palisades	11/21/89	
Prairie Island 2		02/20/92 - AIT and AEOD Human Performance Study Reports.
Salem 1	03/16/82 05/20/89	
Sequoyah 1	05/23/88	
Turkey Point 3	05/28/87	
Vogtle 1	03/20/90	03/20/90 - NUREG-1410, IIT Report.
Waterford 3	07/14/86	
Yankee Rowe	11/16/88	
Zion 2	12/14/85	

[1] Both full-text and summary reports; full-text reports used for HACS evaluation.

Table C.3

Typical Amount of Detail from Various Sources Using Vogtle "Loss of Offsite Power" Event (3/20/90) as an Example

Data Available	DATA SOURCE		
	Summary LER	Full-Text LER	NUREG-1410 - IIT
Type and number of human errors and recovery actions	Initiator: 1	Initiator: 1 Latent: 1 Recovery: 1	Initiator: 1 Latent: 3 Recovery: 2
Type and number of human reliability influences	Organizational Factors: 1	Organizational Factors: 1 Procedures: 1 Training: 1	Organizational Factors: 1 Procedures: 4 Training: 3 Communications: 1 Human Engineering: 2 Design: 1
Plant configuration information	Refueling • Train B RAT & DG out of service (OOS) for maintenance	• After Refueling • Train B RAT & DG OOS for maintenance	• After Refueling • Train B RAT & DG OOS for maintenance • 9 "above" actual Midloop • Charging pump B OOS for valve maintenance • All SG nozzle dams removed, but only SG #1 and 4 primary manways replaced • Pressurizer manway removed • Containment equipment hatch removed

RAT = Reserve Auxiliary Transformer.
DG = Diesel Generator.
OOS = Out of Service.

(and actions). Table C.3 shows that event-based NRC reports contain the most information with respect to all of these information categories and summary LERs the least. This finding influenced the data evaluation strategy of this effort to emphasize the evaluation of full-text LERs and event-based reports.

C.2.3.2 Non-Event Specific Data Sources

Besides using AIT reports, AEOD reports, and LERs to provide event-specific human actions and influences impacting human performance, there are other sources of information to determine non-event specific data associated with the LP&S influences on human reliability. Draft NUREG-1449 (and its supporting details) provided most of the non-event-based information used in the process of characterizing and identifying human actions, errors, and influences. Also, useful non-event-specific information was obtained from NUMARC 91-06 guidelines.

C.2.3.3 Evaluation Process Using HACS

The evaluation of event data (i.e., LERs, AIT reports) with HACS involved six different phases:

- initial review of LERs and AITs during HACS development
- talk-through of HACS application to the review of sample LERs and AIT reports
- in-depth evaluation of LERs and AIT reports with HACS
- group discussion regarding the HACS evaluations of 4 AIT reports
- comparison of all HACS evaluations (i.e., LERs and AIT reports) for common characteristics, general observations, etc.
- independent review of HACS database for consistency and completeness

The HACS framework was found practical in the evaluation of all events, though the level of detail and the completeness of the analysis varied because the content of the reports vary. Certain full-text LERs and more recent reports did provide enough detail to address most of the HACS fields. While

AIT reports contained the most complete event information, the greatest amount of insight was obtained from a combination of an AIT report and a full-text LER for the same event.

The disciplines of human reliability analysis and human factors engineering were important in the identification of human actions and influences impacting human performance. Human actions pertinent to each event could include human errors which initiated events, latent human errors which affected the response to the event, and recovery actions for mitigating the event. In most cases, more than one human action was identified for each event. Similarly, influences specific to each of the identified human actions were identified from the event data. Additional notes and observations which are not accommodated by HACS but are pertinent to potential influences on human performance (e.g., root causes such as management or planning) were stored as comment fields in the HACS database. A tally of all influences identified as impacting human performance, both positively and negatively, was also taken for selected events.

C.2.4 Results and Discussion of Review

This section presents the results of the review of information sources identified in Section 2.3. For each of the sources, there are discussions of the kinds of events, actions, and errors, and of the patterns of influences found to be significant. Table C.4 presents a summary of the significant influences.

Due to differences with respect to their context and format, the discussions of the various information sources vary. For example, for two sources (the LERs and the NSAC report), the analysis uses statistics such as event counts. This usage of statistics is due to the fact that LERs and the like can provide large quantities of data but at a relatively superficial level. In contrast, the AIT and AEOD Human Factors reports are far fewer but provide a greater richness of information. Therefore, the discussion of these events focuses more on the details of the errors and the circumstances surrounding them. Summary event

Table C.4.
Summary of Human Reliability Influences

Influence (Using HPIP Scheme)	Non-event-based Results		Event Analyses			
	NRC[1]	NUMARC[2]	NSAC[3]	AIT[4]	AEOD[5]	LERs[6]
Procedures	(6.6.1.1)	3.3, 3.4	11/47	-4, +3	+3	25/39
Human Engrng.	(6.6.1.1)		13/47	-6, +2	-6, +2	18/39
Training	6.4	3.5	2/47	-5, +3	-3, +1	11/39
Communications			2/47	-5, +1	-6, +1	5/39
Org. Factors	6.2	3.1, 3.3	2/47	-5, +0	-7, +0	2/39
Supervision		3.6	1/47	-1, +0	-2, +1	2/39
Stress	6.3	3.2		-0, +0	-3, +0	0/39
Other[7]	---	---	16/47	-0, +4	-0, +3	0/39

Notes:

[1] Section number in draft NUREG-1449 that describes staff's findings related to this influence (parentheses indicate indirect findings).

[2] Section number in NUMARC 91-06 providing guidance on this influence.

[3] Fraction of loss-of-RHR events discussed in NSAC-156, Appendix A, for which this influence was identified.

[4] Number of times in four Augmented Inspection Team reports where this influence was identified by BNL team as significant ("-" had a negative influence, "+" had a positive influence).

[5] Number of times in five AEOD human factors reports where this influence was identified by BNL team as significant ("-" had a negative influence, "+" had a positive influence).

[6] Relative fraction of events reviewed in this study where this influence was found to be significant.

[7] Includes design issues, mechanical failures, and the effect of extensive technical knowledge.

descriptions are provided for each of these events in the form of tables. Finally, for the non-event data, a summary of the NRC and NUMARC findings is presented.

C.2.4.1 Licensee Event Reports (LERs) Review Results

Section 2.1 of draft NUREG-1449 identifies 42 events associated with PWRs that were reviewed by AEOD as being representative of LP&S problems. The dates of these events range from 1981 to 1990, with the majority being in the range 1987 to 1989.

Full texts of these event reports were requested from the NRC Public Document Room; reports for four events were not found. Reports for the remaining 38 events were obtained, reviewed, analyzed, and entered into the HACS database. Of the 38 reports reviewed, 32 were identified as potentially important to LP&S safety and relevant to the purposes of this study; the six events not reviewed in-depth included deficiencies in power operations safety analyses and an inadvertent reactor protection control rod trip signal during testing while shutdown.

As part of the evaluation of the LERs, a grading of major, minor, or detectable was assigned to each LER as an indication of relative event level of significance. This evaluation was based on the subjective judgement of a person with licensed plant operations and HRA experience. Of the 32 events reviewed, 13 were classified as major, 15 as minor, and four as detectable.

C.2.4.1.1 Evaluation of Events, Errors, and Recovery Actions

The following discussion of the 32 LER events listed in Table C.2 is based on the tabulation of selected findings from the HACS database provided in Table C.5 with additional summarization in Table C.6.

Of the 32 events reviewed, 17 involved loss of shutdown cooling with 12 specifically being loss of RHR. In two cases, the loss of shutdown cooling resulted from loss of AC power, and in two cases

loss of RCS inventory was associated with loss of shutdown cooling. There were two cases of loss of RCS inventory that did not involve loss of shutdown cooling. In addition, seven events comprised loss of some form of electric power but without loss of shutdown cooling. There were no discernable differences between these categories of events for the major, minor, and detectable classifications.

Within the 32 events, a total of 39 errors were identified and analyzed, of which 18 were latent and 21 were active. In addition, 27 recovery actions were analyzed. In 30 cases, human error actively initiated the event, and in nine cases, the human error was a latent error that caused a mechanical malfunction that, in turn, triggered the event. For the major events, six of the 13 events were actively initiated by human error, and seven by latent errors.

Overall, the personnel types most frequently identified as involved in the errors contributing to the events were contractor/vendor personnel (15/39 errors) and maintenance/instrumentation technicians (11/39). However, for the 13 events classified as possessing a major level of significance, the events most frequently involved errors by licensed (8/17) and non-licensed (3/17) operators. For this category, errors by maintenance/ instrumentation technicians (2/17) and contractors/vendors (5/17) were less significant contributors. These distributions are reflected in the most frequent activities during which the errors occurred.

In terms of error modes, errors of omission were reported in only nine of the 39 errors; the remaining 30 were errors of commission. The most frequently occurring errors of commission were the commission of an undesired tasks, analyses or steps (17/39 errors), with the next most frequent being errors of commission from other human factors (such as a faulty RCS level display) (11/39). There were no discernable differences between events judged to have a major level of significance and all events in terms of error modes.

The error types most frequently identified overall were mistakes (26/39 errors) of which most (14) resulted from faulty or inadequate procedures with eight more resulted from faulty diagnosis. Of the 13

Table C.5.
Tabulation of Selected Full-Text LER Findings from HACS Evaluation

Event			Error (39 Total)					Recovery (27 Total)		
ID	Des	Sig	Pr	Mo	Ef	Ty	Inf	Lo	Ti	Pr
1	LEP	d		CA	A	MP	PWI,TUI	--	--	--
2	LOI	M	VC	CH	LR	MD	E	--	--	--
3	ESF	d	MT	CT	A	MP	PWI	B	24	MO
4	BDU	m	VC	CH	A	MD	HHI	B	230	MO
5	LOI	m	VC	CH	LT	MP	PFD,TUI,C	I	3	LO
6	LEP/LSC	M	VC	CH	LR	MD	HND	O	45	LM
7	LSC	M	LO	CT	A	SW	PFM,HHA,T	I	60	LO
8	LEP	m	MT	CH	A	SA	PWI,HWC,TUI,C	B	5	LM
9	ESF	d	MT	CH	A	SA	PWI,HWC	--	--	--
10	LSC	M	MO	CT	A	MP	PND,C,SL,O	B	25	MO
11	LSC	m	VC	CH	LR	MD	HND	I	N	LO
12	LSC	M	VC MT	CH OT	LR LR	MD MP	E PFD	B	24	MO
13	LEP	M	VC	CH	A	SA	PNO,HHM,TNT	B	59	MO
14	LSC	M	LO	CT	A	MP	PWI,HHI	B	75	MO
15	LSC	m	MT VC	CT CT	A LR	MP MP	PWI,HHI PFD	B	27	MO MT
16	LSC	m	VC	CH	A	SA	E	B	12	MO
17	LOI/LSC	M	LO SO	CT	A	MP	PWI,HHI	B	88	MO
18	LOI/LSC	m	NO	CT	A	MM	C,S	B	83	MO
19	LSC	m	MT	CT	A	SA	PWI	B	N	MO
20	LEP	m	MT	CT	A	MP	PWI,TUP	I I	N N	LO LO
21	LCP	m	VC	OT OH	LT LT	MD MP	HHI PWI	B	190	MT MO
22	LEP	m	MT	CT	A	MG	PWI	--	--	--

Event			Error (39 Total)					Recovery (27 Total)		
ID	Des	Sig	Pr	Mo	Ef	Ty	Inf	Lo	Ti	Pr
23	LSC	m	VC	OT	LR	MD	HND	B	39	MO
24	LSC	M	LO NO	OT	LR A	MP MM	PNA,HHI,HWH PWI,TUI,C	O	241	MO
25	LEP	m	VC MT	CH OH	A LR	SA MP	HNR, E PWI	I	65	LO
26	EDG	d	VC	OH	LR	MD	E	--	--	--
27	LSC	M	LO LO	CT CT	LR LR	MP SA	PFD,TUI HHI,HHM	B	18	MO
28	LOP/LSC	M	VC VC	CT OH	A LR	SA MG	T,O P,E	O	36	SO NO
29	LSC	M	MO	CT	LR	SE	PFD,HHI	B	14	MO
30	LOI	M	MT	CA	LR	SE	PFD	B	127	MO
31	LEP/LSC	m	LO	CT	A	SA	PND,TUI	I	9	LO
32	LSC	m	MT	CT	A	SA	PWI,TUI	--	--	--

Des = Event Description
BDU = Boron Dilution
EDG = Emergency Diesel Generator inadvertent start
ESF = Engineered Safeguard Features Actuation
LCP = Loss of Charging Pump
LEP = Loss of Electrical Power
LOI = Loss of Reactor Coolant Inventory
LSC = Loss of Shutdown Cooling

Sig = Level of Significance - Relative
M = Major
m = Minor
d = Detectable

Pr = Personnel Involved
LM = Licensed Operator and Maintenance/Instrumentation Technician
LO = Licensed (Control Room) Operator
MO = Licensed and Non-Licensed Operators
MT = Maintenance/Instrumentation Technician
NO = Non-Licensed (Equipment) Operator
SO = Senior Licensed Operator
VC = Vendor/Contractor

Mo = Error Mode
CA = Commission of Undesired Adjustment or Calibration
CH = Commission (Other Human Factors)
CT = Commission of Undesired Task, Analysis, or Step
OH = Omission (Other Human Factors)
OT = Omission of Task, Analysis, or Step

Ty = Error Type
M = Mistake
MG = Mistake, Inadequate Planning
MP = Mistake, Inadequate Procedure
MD = Mistake, Faulty Diagnosis
MM = Mistake, Miscommunication
S = Slip
SA = Slip, Inadvertent Actuation/Disabling
SE = Slip, Incorrect Execution Mistake
SW = Slip, Selection of Wrong Item

Ef = Error Effect
A = Active
L = Latent
LR = Latent, Discovered Prior to Startup
LT = Latent, Discovered During/After Startup

Inf = Error Influence
C = Communications
E = Engineering Design
H = Human Engineering
HH = Human Engineering (HE), Human-Systems Interface (HSI)
HHA = HE, HSI - arrangement, placement less than adequate (LTA)
HHI = HE, HSI - instrument displays LTA
HHM = HE, HSI - monitoring alertness
HND = HE, non-tolerant system - errors not detectable
HNR = HE, non-tolerant system - errors not recoverable
HWC = HE, work environment - cramped quarters
HWH = HE, work environment - hot/cold
O = Organizational factors
P = Procedures
PFD = Procedure followed incorrectly - details LTA
PNA = Procedure not used - not available or inconvenient to use
PND = Procedure not used - difficult to use
PNO = Procedure not used - no procedure
PW = Procedure wrong/incomplete
PWI = Procedure incomplete - situation not covered
S = Supervision
SL = Supervision during work - LTA
SN = Supervision during work - none
T = Training
TNT = Training - non-task, not analyzed
TUI = Training - understanding LTA, instruction
TUP = Training - understanding LTA, practice/repetition

Lo = Recovery Location
B = Both Inside and Outside Control Room
I = Inside Control Room
N = Not Available
O = Outside Control Room

Ti = Recovery Time in Minutes

Table C.6.
Summary Information from Selected Full-Text LER Findings

Event Description Summary	
13	Loss of Shutdown Cooling
7	Loss of Electrical Power
2	Loss of Electrical Power and Loss of Shutdown Cooling
2	Loss of Reactor Coolant Inventory and Loss of Shutdown Cooling
3	Loss of Reactor Coolant Inventory
2	Engineering Safety Features Actuation
1	Emergency Diesel Generator Inadvertent Start
1	Loss of Charging Pump
1	Boron Dilution of Reactor Coolant

Event Initiator Summary	
20	Human Error
12	Not Human Initiated

Error Effect Summary	
21	**Active**
(7 for Major Level of Significance Events)	
18	**Latent**
(10 from Major Level of Significance Events)	
15	Latent, Discovered Prior to Startup
3	Latent, Discovered During/After Startup

Personnel-Involved Summary	
39	**Selected Errors**
15	Vendor/Contractor
11	Maintenance/Instrumentation Technician
9	Licensed (Control Room) Operator
4	Non-Licensed (Equipment) Operator
1	Senior Licensed Operator
27	**Recovery Actions**
26	Licensed (Control Room) Operator
18	Non-Licensed (Equipment) Operator
4	Maintenance Technician
1	Senior Licensed Operator

Error Type Summary	

26   **Mistakes**
  (11 from Major Level of Significance Events)
  14   Mistake, Inadequate Procedure
   8   Mistake, Faulty Diagnosis
   2   Mistake, Inadequate Planning
   2   Mistake, Miscommunication
13   **Slips/Lapses**
  (6 from Major Level of Significance Events)
  10   Slip, Inadvertent Actuation
   2   Slip, Incorrect Execution Mistake
   1   Slip, Selection of Wrong Item

Human Reliability Influences Summary

25   **Procedures**
  (including 14 procedure wrong or incomplete/situation not covered; 6
  procedure followed incorrectly/details less than adequate)
18   **Human Engineering**
  (including 7 human-system interface instrument displays less than
  adequate)
11   **Training**
  (including 7 training/understanding less than adequate)
  6   Engineering Design
  5   Communications
  2   Organizational Factors
  2   Supervision
  0   Stress

Error Mode Summary

30   **Error of Commission**
  (13 from Major Level of Significance Events)
  17   Commission of Undesired Task, Analysis, or Step
  11   Commission (Other Human Factors)
   2   Commission of Undesired Adjustment or Calibration
   0   Commission of Undesired Alarm Response
9   **Error of Omission**
  (4 for Major Level of Significance Events)
  5   Omission of Task, Analysis, or Step
  4   Omission (Other Human Factors)
  0   Omission of Alarm Response
  0   Omission Within Allotted Time
  0   Omission of Adjustment or Calibration

slips identified, ten were attributed to inadvertent actuation. In terms of error types, there were no discernable differences between events judged to have a major level of significance and all events. Recovery by human intervention in most cases where analyzed involved actions from both outside and inside the control room (17/27). Only seven events were recovered by human actions taken inside the control room alone; only three were recovered exclusively from outside the control room. No significant differences between all the events and only those considered major were detected in this regard.

The error types most frequently identified overall were mistakes (26/39 errors) of which most (14) resulted from faulty or inadequate procedures with eight more resulted from faulty diagnosis. Of the 13 slips identified, ten were attributed to inadvertent actuation. In terms of error types, there were no discernable differences between events judged to have a major level of significance and all events.

Recovery by human intervention in most cases where analyzed involved actions from both outside and inside the control room (17/27). Only seven events were recovered by human actions taken inside the control room alone; only three were recovered exclusively from outside the control room. No significant differences between all the events and only those considered major were detected in this regard.

C.2.4.1.2 Evaluation of Influences

As summarized in Table C.3, the influences most frequently identified as contributing to the human performance problems in the 39 errors were procedures (identified with 25 errors), and human engineering (18 errors). Within procedures, the most common problem was that the procedures were wrong, incomplete, or did not cover the situation (14 errors). One example of this category is the loss of RCS makeup at ANO-1 (5/4/88), where an inadequate work-package procedure omitted the requirement for a leak test to be performed following replacement of two redundant water level

transmitters; this led to air-binding of the charging pumps. A second example is the loss of emergency service water (ESW) at Shearon Harris, Unit 1, on 10/11/87, when loss of offsite power occurred during testing of the ESW valves. This led to loss of ESW because the test procedure provided no instructions on how the operators should terminate the test if a loss of offsite power event occurred during testing.

Other contributors in this category were: procedures followed incorrectly (6 errors) and procedures not used (four errors). The most frequent cause of procedures being followed incorrectly was that the details were less than adequate. The most frequent cause of procedures not being used was because the procedures were difficult to use, or, in one case, procedures did not exist.

In the category of human engineering, the human-machine interface was identified in 18 errors. Of these, seven were associated with instrumentation displays. Other human-machine interface problems were associated with labeling, work environment (hot/cold and cramped quarters), and non-fault tolerant designs.

Training was identified as a contributor in 11 errors and communications was identified in five errors. It was often difficult to identify the more detailed contribution of training because of the level of details in the LERs. Similarly, with communication problems, the specific form of the influence could often not be identified.

Many errors had several influences identified. Seventeen errors had one influence, 15 had two influences, five had three influences, and two had four influences. The most frequent combinations were inadequate or incomplete procedures, with human engineering deficiencies (instrumentation or cramped quarters) or with inadequate training.

Of the events classified as possessing a major level of significance, most (8/13) identified procedural influences associated with "not used" or "followed incorrectly". Only three of 15 events classed as a minor and none of the four events classed as detectable had this influence identified. Most of the minor events (8/15) and detectable events (3/4)

identified "wrong" or "incomplete" procedural influences; only two major events identified this influence. There were no other apparent differences between the levels of significance in terms of human reliability influences.

C.2.4.1.3 Summary of Results

There is an apparent difference in the nature of the events classed as major compared with the events overall. The prototypical overall event is associated with errors by technicians (plant staff or contractors) working outside the control room performing tests. While performing this work, the technician makes an error of commission, which is a result of a procedural inadequacy (often, the procedure does not cover some particular step or contingency occurring in the test) and inadequate training. The deficiency in the procedure is often revealed when a situation is encountered (e.g., other equipment failure or human error, or an operation taking place in some other part of the plant) that was not in the expectation of the procedure developer. These errors of commission result in an immediate consequence, such as a loss of electric power that results in loss of shutdown cooling. The event is recovered by actions inside the control room, with some actions taken outside the control room (e.g., rack in breakers or open valves manually) to recover equipment taken out of service for maintenance or due to an earlier latent error.

For the events considered major, the prototypical event is different. It is much more likely that the errors are committed by the control room operators while performing some task associated with RCS level and inventory control. This error is as likely a slip (i.e., a human error where what is performed was not intended) or a mistake (i.e., a human error where the intention was erroneous, but is purposefully executed), with temporary level instrumentation often playing a key role. The effect of the error is to lead to loss of shutdown cooling, sometimes in association with inadvertent loss of RCS inventory through multiple RCS drain paths. In the case of the major events, typically several human reliability influences are involved. These could include inadequate instrumentation (e.g., level indication), inadequate procedures (e.g., no planning

for failures or requiring complex calculations), inadequate training, and (sometimes) miscommunications between plant personnel as to the plant status. In many cases, recovery requires prolonged actions outside the control room to restore mechanical equipment, such as venting RHR pumps following air-binding.

C.2.4.2 NSAC-156, Residual Heat Removal Experience Review and Safety Analysis Review Results

The NSAC-156 report summarizes the experience of loss of RHR events during LP&S operations at U.S. PWR plants between 1982 and 1989. This report represents an update of an earlier report, NSAC-52, which provided a similar evaluation for loss of RHR events up to 1981. The primary data source for the NSAC evaluation was LERs, supplemented by INPO and AEOD reports, though the events listed do not identify the subject plant. The greatest level of detail for the events described in this report corresponds approximately to that of summary LERs; in many cases, it was not possible to identify fully the information required for the HACS database. Therefore, the information presented in this section should be considered as being somewhat tentative.

Appendix A of the NSAC-156 report identified 49 events involving loss of RHR capability (partial and complete) in the period 1985 to 1989. This time window is the period during which LER reporting requirements have remained relatively constant. Of the 49 events, two were the result of design deficiencies and were not considered further. The summary descriptions provided in NSAC-156 of the remaining 47 events were studied for the activities, errors and contributions of the human reliability influences. Because of the lack of detail, only about 22 contained sufficient information about the specific errors, activities, and recovery data for evaluation. However, information concerning the influences was obtainable from all 47.

Reviews

C.2.4.2.1 Evaluation of Events, Errors, and Recovery Actions

By definition, all of the 47 events involved loss of RHR cooling. RHR valve failures (failing to open or failing closed) were involved in 19 of these events; 14 were caused by RHR pumps tripping or failing to start; 5 involved failures of other (non-RHR) valves; 4 were the result of errors in controlling RCS level; and 4 were the result of other failures.

The events were initiated by mechanical failures in 29/47 of the cases evaluated. Maintenance technicians initiated 11/47 of the events, and operations personnel initiated the remaining 8/47. Only in 13 of the 47 events could errors be identified. Of these 13 event descriptions, 22 human errors were identified, all of which occurred outside the control room. Only one event involved an error of omission, with the remaining 21 identified as errors of commission. Of these 22 errors, 15 were mistakes (usually procedural deficiencies) and seven were "slips" (often accidental electrical contacting during tests). In terms of their latent/active effect, 4/22 were latent failures and 18/22 were active failures.

Recovery times were identified in 22 events. These times were compatible with the time distribution developed from the LER review described in Section C.2.4.1.1.

C.2.4.2.2 Evaluation of Influences

The largest contribution to the 47 loss of RHR events was from human engineering, with the greatest fraction of those events involving inadequacies in the man-machine interface, and the balance from the work environment. The most common man-machine interface problems were inadequate temporary level instrumentation and difficulties in observing annunciator indications during the outage condition. Problems in the work environment were principally reflected in inadvertent contact with relays or control equipment while performing Instrumentation and Control (I&C) or electrical maintenance or testing.

The next largest overall contribution to the 47 loss of RHR events was from procedures, with the largest fraction being attributable to an incomplete procedure or the wrong procedure for the application. In most cases, it seemed that conditions were encountered that were not anticipated in the procedures, such as equipment not being found "as expected" or plant configurations existing that, when the procedure was implemented, led to loss of RHR (e.g., electrical interconnections).

Other human reliability influences contributed minimally to the events evaluated. In the "other" category, the greatest contributions were from mechanical failures and design errors. It was not possible to identify the specific influences in four events due to insufficient information.

C.2.4.2.3 Conclusions

In conclusion, because of the incomplete information presented in the event summaries in NSAC-156, it is difficult to draw clear conclusions about the patterns of errors and actions from their review. However, most errors were errors of commission, resulting from mistakes induced by inadequate man-machine interface, poor procedures or inadequate instrumentation.

C.2.4.3 Augmented Inspection Team (AIT) Evaluations Review Results

As shown in the comparison given in Table C.3 of the information contained in an LER to that in an event-based report, the four AIT reports which were evaluated (see Table C.2) contained more information and detail than that contained in the full-text LERs reviewed. Consequently, while each of the AIT reports was coded into HACS, the important information contained in the AIT reports were details on plant conditions and defenses, human actions and errors, and influences and not the statistics on types of events and human errors, error modes, error types, error locations, etc. To the extent possible, details judged to be important to human reliability and performance have been extracted from the AIT reports and shown in Tables C.7 through C.10.

Table C.7
Plant: Braidwood Unit 1 Event: LOCA with Loss of RHR for 131 minutes   Event Date: 12/01/89

Situation	Acts	Defenses	Conditions	Influences
1. Two reactor coolant pumps running. 2. Little decay heat (after refueling); operators drawing pressurizer bubble. 3. Occurred in middle of night. 4. RHR pump suction relief valve (in non-operating loop) spuriously opened and stayed open. 67,000 gallons of RCS inventory releated.	1. Earlier maintenance of RHR valve deficient. 2. Extended time taken to locate and isolate leak source (131 minutes). Operators initially shut down non-leaking loop, based on engrained belief that operating equipment fails, not standby equipment.	1. Operators adequately aware of plant conditions (extensive indications for RCS level, RHR flows, pump conditions, etc). +*Human Engineering* 2. Training directly relevant to Mode 5 LOCAs provided. +*Training* 3. Communications between CROs and plant personnel helped identify problem. +*Communications*	1. Inadequate cleanliness in maintenance work area resulted in mechanism sticking. -*Human Engineering* 2. Procedure ambiguous about valve nozzle setpoint; did not require verification of setpoints. -*Procedures* 3. Valve work package did not match maintenance procedure requirements. -*Organizational Factors* 4. Steps in LOCA diagnosis procedure not directly useful for Mode 5 LOCAs (time consuming). AOPs discarded and EOP not used during event as not relevant. -*Procedures* 5. Initial misdiagnosis of leaking loop (operators expectations of operating loop to leak, not standby loop). -*Training*	Procedures: -2 Training: -1; +1 Communications: +1 Organizational Factors: -1 Human Engineering: -1; +1 Supervision: Stress: Design:

Source: AIT Report 50-456/89-03

Table C.8 Plant:
Diablo Canyon Unit 1Event: Loss of Essential Loads for 4 hours, 53 minutes

Event Date: 03/07/91

Situation	Acts	Defenses	Conditions	Influences
1. Mobile crane causes short-to-earth of the only remaining unit 1 feed (cross-feed from unit 2).	1. Crane moved to within 3 feet of 500kV power line, in breach of safety rule. Foreman assumed line was deenergized.	1. 3 EDGs started and loaded as designed.	1. No safety training provided to crane operator (recent promotion). *-Training*	Procedures:
2. EDG starts but some essential loads (HVAC, CR lighting) powered from non-essential buses.	2. Some essential loads had been swtiched to non-essential buses without operators' knowledge.	2. All RHR and CCW systems available for reactor cooling.	2. Foreman assumed line deenergized for outage. Thought of phoning operators but was distracted. *-Training, Communications*	Training: -2; +1
3. Low decay heat level.		3. Containment evacuated OK. *+Training*		Communications: -2
4. Two new fuel assemblies in transfer.		4. Fuel assemblies in transfer relocated under manual control OK. *+Technical knowledge*	3. No administrative control over movement of vehicles in switchyear. *-Organizational Factors*	Organizational Factors: -2
5. "Usual" crane location blocked by other equipment.		Operators opened doors of 1E electrical equipment rooms, etc., for cooling. *+Technical knowledge*	4. No coordination with operations for transfers of essential electrical loads. *-Organizational Factors, Communications*	Human Engineering:
				Supervision:
				Stress:
				Design:
				Technical knowledge: +2

Source: AIT Report.

Table C.9 Plant:
Oconee Unit 3 Event: Loss of RHR for 18 minutes

Event Date: 03/08/91

Situation	Acts	Defenses	Conditions	Influences
1. Day 24 of refueling outage (decay heat low).	1. Blind flange installed in wrong line.	1. RCS refilled by gravity; no pumps needed. **+Design**	1. Erroneous informal location label; used as reference by installers & checkers of location of blind flange. **-Human Engineering, Organizational Factors**	Procedures: -1; +1
2. Cooling via single loop of RHR.	2. Technicians manually opened RHR/LPI sump suction valve before LPI pump was stopped by operators.	2. Adequate level indication working & used by operators. **+Human Engineering**	2. Formal location labels for penetrations difficult to access. **-Human Engineering**	Training: -1
3. Other outage evolutions masked early symptoms.	3. Incomplete containment evacuation.	3. AOP available and used for loss of RHR pump when shutdown. **+Procedures**	3. Most frequently used job aids for technicians (schematics & procedures) provided no specific location information (in fact, schematic was unintentionally misleading). **-Human Engineering**	Communications: -1
4. Radwaste monitors out-of-service for replacement.			4. Miscommunication between test technician & CROs led operators to be unaware that valve was being opened. Procedure did not require coordination. **-Communications, Procedures**	Organizational Factors: -2
			5. No compensating measures were required or taken for radwaste monitors being out of service. No training for radiation events during shutdown was provided. **-Organizational Factors, Training**	Human Engineering: -3; +1
				Supervision:
				Stress:
				Design: +1

Source: AIT Report 50-287/91-008.

C-23

Table C.10 Plant:

Prairie Island Unit 2 Event: Loss of RHR for 21 minutes   **Event Date: 02/20/92**

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

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

C.2.4.3.1 Evaluations of Events, Errors, and Recovery Actions

The evaluation of events discussed in the AIT reports include three loss of RHR events and one loss of essential electric supplies. All four AIT events were initiated by human errors. The loss of electric power event (Diablo Canyon Unit 1) (03/07/91) and two of the loss of shutdown cooling events (Oconee Unit 3 (03/08/91) and Braidwood Unit 1 (12/01/89) were initiated outside the control room (two active and one latent error, respectively).

The third loss of shutdown cooling (Prairie Island Unit 2 (02/20/92)) was initiated in the control room (active error).

In each case, there were multiple errors made. Commonly, latent failures existed such that, when some final error occurred, the incident resulted. For example, in the case of Oconee, a blind flange was installed on the wrong sump line; inadequate maintenance on a valve at Braidwood Unit 1 led to a LOCA; and at Diablo Canyon Unit 1, some essential electrical loads had been switched, without the operators' knowledge, to non-essential buses.

C.2.4.3.2 Evaluation of Influences

The errors, actions, and influences for each of these four events are summarized separately in Tables C.7 through C.10, and the overall set of influences is summarized in Table C.4.

For the three events involving loss of RHR, two involved significant mistakes associated with negative influences: poor labeling and procedures. In the loss of RHR at Prairie Island Unit 2, procedures for the lowering of water level for mid-loop operations required extensive hand calculations with minimal computational aids.

In each of the four events, training played a contributing role. In most cases, the licensee had not provided training for the activities being performed, as in the case of the calculations of RCS level at Prairie Island Unit 2 and in the diagnosis of a leaking RHR loop at Braidwood Unit 1. Also in the case of Oconee, no training in radiation control

for shutdown events was provided, even though radiation monitors were scheduled to be taken out of service.

Communications was also an issue in three of the four events, including the loss of essential electrical supply event at Diablo Canyon Unit 1 and the loss of RHR events at Prairie Island Unit 2 and Oconee Unit 3. The communications failures were largely a lack of timely inquiries of plant status, or, in the case of Oconee Unit 3, confusion between the control room and technicians outside the control room as to when equipment would be operated.

Organizational factors played a significant role in three of the events. The specific problems included the lack of access control to the switchyard at Diablo Canyon Unit 1, the lack of double checking assurance for sign-offs of the location of the blind flange at Oconee Unit 3, and the lack of coordination of the valve work package with procedures at Braidwood Unit 1.

Human engineering was the most frequent contributor to human performance in the four AIT reports reviewed. In the Oconee Unit 3 event, the basic problem was poor labeling of the sump penetrations such that almost everyone was similarly misled as to which penetration was the affected one; this labeling reduced the redundancy of the checkers to zero. Other examples were the poor temporary level instruments at Prairie Island and poor housekeeping in the maintenance work area at Braidwood Unit 1.

All the events exhibited the effects of multiple influences, ranging from five (Braidwood Unit 1) to eight concurrent influences (Oconee Unit 3). There was no consistent pattern of combination of influences. In addition, Tables C.7 through C.10 also provide examples of influence attributes, both negative and positive, which impacted human performance. These examples included:

Procedures:

- *inapplicable or irrelevant EOPs* for LOCA response (Braidwood Unit 1)

Reviews

- *lack of clear prerequisites* for instrumentation availability for draindown (Prairie Island Unit 2)

Training:

- *training directly relevant* to mode 5 LOCAs *provided* (Braidwood Unit 1)
- *no* safety *training provided* to crane operator (Diablo Canyon Unit 1)
- *no training* for radiation events during shutdown (Oconee Unit 3)

Communications:

- *miscommunication between* test *technician and CROs* led operators to not being aware that valve was being opened (Oconee Unit 3)
- *no communications* with shift operations management led to lost opportunities to correct errors in level control (Prairie Island Unit 2)

Organizational Factors:

- valve *work package did not match maintenance procedure requirements* (Braidwood Unit 1)
- *no administrative control* over vehicle movement in switchyard and *coordination with operations* for transfers of essential electrical loads (Diablo Canyon Unit 1)

Human Engineering:

- *difficult access* to formal local labels for penetrations and *use of an erroneous informal* location *label* (Oconee Unit 3)
- *poor environment* for reading RCS level instrumentation (Prairie Island Unit 2)

C.2.4.3.3 Summary of Results

Evaluations of the AIT reports are consistent with the full-text LER evaluations in that all types of human errors and actions occurred: initiators, pre-accident errors, and recovery actions. As shown in

Table C.4, the identification of procedures, training, communications, organizational factors, and human engineering as important contributors to events in AIT reports is also consistent with the findings of the LER evaluation. In addition, multiple influences were identified in both LERs and the AIT reports. However, the information available in the AIT reports also allowed the identification of influences which contributed positively to events, i.e., correct procedures or good communications contributed to the mitigation or early detection of an event. In addition, the AIT reports contained more detailed information which, in particular, has been interpreted as attributes of influences which caused either positive or negative impacts on human actions or errors.

C.2.4.4 AEOD Human Factors Evaluation Review Results

Like the AIT reports, the primary usefulness of the AEOD reports to this project stems from the depth of detail provided about human actions and errors and their associated influences. Similarly, the details judged to be important to human reliability and performance have been extracted from the AEOD reports. These reports provide the results on-site evaluations of the roles human factors issues played in a series of events at nuclear power plants from 1990 to 1992 which are summarized and analyzed as shown in Tables C.11 through C.15. The five events investigated in the AEOD reports have not been coded into HACS.

C.2.4.4.1 Evaluations of Events, Errors, and Recovery Actions

An NRC Office of Analysis and Evaluation of Operational Data (AEOD) contractor performed on-site evaluations of the roles human factors issues played in a series of events at nuclear power plants from 1990 to 1992. Included in these were five events that occurred at PWRs during low power and shutdown operations. These events were at: Catawba Unit 1 (3/20/90), Braidwood Unit 1 (10/8/90), Oconee Unit 3 (3/8/91), Crystal River Unit 3 (12/8/91), and Prairie Island Unit 2 (2/20/92). Summaries of these events, including the actions, errors, and influences are presented in Tables C.11

Table C.11 Plant: Catawba Unit 1 Event: Inadvertent RCS & RHR Over-pressurization Event Date: 03/20/90

Situation	Acts	Defenses	Conditions	Influences
1. Completed 7 week refueling outage and initial fill and vent (Mode 5).	1. Integrated Scheduling failed to anticipate the need for RCS pressure transmitters for initial RCS pressurization to 100 psig.	1. PRT level indication available and used by operators to detect a problem initially. Also, both RHR pump discharge pressure and CVCS letdown pressure indicators rose in response to RCS pressure rise. (However, not monitored by operators.) +*Design*	1. Scheduling error left three RCS pressure instruments inoperable. Due to this event, specific change to the controlling procedure for shutdown to require signoff of RCS pressure instrument operability prior to setting head. Also, changes made in scheduling mechanisms with review. -*Organizational Factors, Procedures*	Procedures: -2
2. Fill and vent performed for 1-2 hours longer than usual.	2. Operators allow RCS pressure to increase above 100 psig.	2. RCS systems engineer recalls NRC Information Notice on interfacing systems LOCAs. +*Other*	2. IAE responsible for CR instruments but do not their practice to hang tags on inoperable equipment - no formal procedure or permanent CR record. (Operators had instructions not to hang their own tags.) -*Organizational Factors, Procedures*	Training: -2
3. Pressurization of RCS initiated - PZR fill topped off until water exited the PORVs.	3. Operators adjust charging and letdown flow to reduce RCS pressure and isolate RHR B train.		3. Operators did not use an accepted rule of systems monitoring - looking at all affected systems when a significant change in operating conditions occurs. (Looked at RCS indicators only.) -*Training*	Communications: -1
4. RHR A & CVCS B in operation.				Organizational Factors: -2
5. Sole RCS pressure indication used by operators inoperable (but unknown to operators).			4. Shift briefing did not discuss significance of continued venting. -*Communications*	Human Engineering:
6. Additional fill and vent time may have caused RCS pressure to rise more quickly than anticipated (or previously).			5. Operators did not use principle of change analysis on procedure execution to anticipate the unforeseen effects of continued venting. -*Training*	Supervision:
				Stress:
				Design: +1
				Other: +1

Source: AEOD Human Factors Team Report, May 1990.

Date: 10/04/90

Table C.12 Plant: Braidwood Unit 1 Event: Loss of Reactor Coolant

Situation	Acts	Defenses	Conditions	Influences
1. Cold shutdown - RCS is at approximately 180 degrees and 360 psig. 2. Occurred at 1:20 am (Shift 1).	1. Technical staff engineering personnel decide to perform two procedures simultaneously. *Organizational Factors* 2. Valve 1RH8702B opened before confirmation received that associated valve was closed - resulted in surge of flow through vent and burst tygon tubing attached to valve. 3. 1RH8702B closed by Unit 1 Nuclear Station Operator (NSO).	1. Both procedures have appropriate steps and checks (individually). *+Procedures*	1. Insufficient information transferred during shift turnover/briefing resulted in Shift CR Engineer (SCRE), Unit 1 Nuclear Station Operator (NSO), Shift Engineer (SE) and Shift Advisor (SA) not being aware that two procedures were going to be performed together. Auxiliary NSO knew but did not inform others. *-Communications* 2. Performance of both procedures simultaneously allowed but no formal procedure for doing so (and never done before). Also, there were no redundancies or independent checks on the two technical staff engineers' performance by operations personnel and there were no system redundancies or checks in place to catch and prevent any errors associated with the coordination and performance of the two procedures in parallel. *-Organization Factors, Procedures* 3. Technical staff engineers performing tests had been working 17 and 19 hours, respectively. *-Stress* 4. Confirmation not received on closing 1RH8702B before opening RH028B. *-Procedures* 5. SCRE, SE, and Unit 1 NSO not monitoring activities in CR (i.e., normal command, control, and communication not present). *-Supervision, Communications*	Procedures: -2; +1 Training: Communications: -2 Organizational Factors: -2 Human Engineering: Supervision: -1 Stress: -1 Design:

Source: AEOD Human Factors Study Report, October 1990.

Table C.13 Plant: Oconee Unit 3 Event: Loss of Shutdown Cooling   Event Date: 03/08/91

Situation	Acts	Defenses	Conditions	Influences
1. 24th day of refueling outage - fuel handling completed.	1. Blind flange mistakenly installed in penetration from valve 3LP-20 rather than 3LP-19.	1. Sump level indications and alarms, RV level alarms, etc. working and used by operations. +Human Engineering	1. Work request for installing flange and test procedure did not use penetration numbers. -Human Engineering	Procedures: -2; +1
2. RHR A pump providing SDC.	2. Technicians manually opened suction valve 3LP-20 before LPI pump stopped by operators.	2. AOP available and used for loss of RHR pump when shutdown. +Procedures	2. Flow diagram and note handwritten on the wall used to locate penetration - contrary to site policy. Both technicians and checkers used the informal location labels. -Human Engineering, Organizational Factors	Training: +1

Communications: -1; +1

Organizational Factors: -1 |
| 3. Incore instrumentation not yet connected - RCS temperature determined from RHR temperature detector on pump suction. | 3. Operators decided to close valves 3LP-19 and -20 because they thought that one of the valves might be open, permitting the BWST to be drained to the emergency sump. | 3. Combination of training on system procedures and operator awareness of maintenance activity was positive factor in recovery. +Training, Communications | 3. Formal location labels difficult to access. -Human Engineering | Human Engineering: -3; +1

Supervision: |
| 4. Equipment and hatches closed. | 4. Vented and re-started RHR pumps. | | 4. Miscommunication between operator and I&E technician re: when LPI pump will be stopped. No procedural requirement for coordination. -Communications, Procedures | Stress:

Design: |
| 5. Radiation monitors removed from service and scheduled for replacement. | 5. Evacuation of containment not complete - notification of health physics technicians not prompt. | | 5. AOP for loss of SDC/RHR not followed explicitly re: evacuation and should be modified to direct more prompt evacuation. -Procedures | |

Source: AEOD Human Factors Study Report, May 1991.

Table C.14 Plant: Crystal River Unit 3Event: Loss of RCS Pressure

Situation	Acts	Defenses	Conditions	Influences
1. Plant startup after short maintenance outage - at ~10% power.	1. Operators increase power to correct what they perceive as over-cooling.	1. Automatic reactor trip and ESFAS actuation. *+Design*	1. Inadequate indication of PZR spray flow line valve. *-Human Engineering*	Procedures: -2
2. Midnight to 8 am shift - event initiated at 3 am (noted in AEOD report as time "when human performance tends to be at its lowest level").	2. ESFAS initially bypassed by operators due to expectation that RCS pressure decrease would be brought under control.	2. RCS pressure control accomplished with control of HPIS flow. *+Design*	2. Significant actions took place between 3 and 4 a.m. *-Stress*	Training:
3. Event initiated by failure of actuator for PZR spray flow control valve RCV-14 - leaving valve partly open but with position indicator lights showing valve fully closed. (Resulting spray cause decreasing RCS pressure transient.) The valve failed to re-seat due to missing key.	3. Operators increase RCS pressure through control of HPIS in order to avoid inadequate sub-cooling margin.		3. Operators did not use procedures in response - used recall of procedures and plant behavior - and violated procedures in bypassing Engineered Safeguards (ES). *-Procedures*	Communications: -1 Organizational Factors: -2 Human Engineering: -1
4. Reactor trip on low RCS pressure.	4. PZR spray line isolation (block) valve closed - terminating pressure decrease.		4. Procedures did not give guidance: (1) on ES bypass prior to actuation or (2) on the choice between avoiding safety valve lift or assuring an adequate sub-cooling margin. Procedures not written to assure execution of applicable steps. *-Procedures*	Supervision: Stress: -2 Design: +2
	5. Late notification of NRC. *Organizational Factors*		5. Limited time for decision-making (i.e., 18 minutes from detection of decreasing pressure to reactor trip). *-Stress*	
			6. Operator performance could have been improved by closer adherance to general principles for command, control, and communications (i.e., operators took actions independent of each other and supervisors without verifying appropriateness of actions. *-Communications, Organizational Factors*	

Source: AEOD Human Performance Study Report, January 1992.

Table C.15 Plant: Prairie Island Unit 2 Event: Loss of RHR

Event Date: 02/20/92

Situation	Acts	Defenses	Conditions	Influences
1. Two days into refueling outage.	1. Problems calculating RV level and inaccuracies introduced by rounding off.	1. Alarms for RHR low suction pressure, low motor-amp, etc. lead to pump trip. *+Human Engineering*	1. Operators not trained on using draindown procedure (mid-loop training not available on simulator) and performing the conversion calculations in situations of high nitrogen pressure. *-Training*	Procedures: -2; +1
2. RV draining to mid-loop started.	2. Operators over-reduce RCS level, causing RHR pump vortexing. (Caused in part by the Shift Manager's faulty calculation of the draindown time.)	2. AOP and EOP lead to recovery. *+Procedures*	2. Draindown procedure contained sparse information on nitrogen pressure control, did not include a conversion factor for calculating the draindown time, and did not require logging of the actual water level (to provide trending information). *-Procedures*	Training: -1
3. Operators performing draindown were extra personnel from another shift.	3. RV level restored using charging pumps and SDC re-established.	3. Command and coordination of the operating crew during recovery from the event was a positive factor in the crew's response - shift supervisor in direct command of the procedures. *+Supervision*	3. The draindown crew was inexperienced, not sure who was in charge, and received infrequent supervision by the Shift Manager and Shift Supervisor because they were assumed to be experienced enough to proceed with the procedure. *-Supervision*	Communications: -1
4. Newly installed electronic level instrumentation considered operable but reading off-scale.			4. Operators did not communicate their concerns to the supervisors. *-Communications*	Organizational Factors:
5. Tygon tube only instrument providing usable level information during draindown.			5. Guidance in draindown procedure did not compensate for inexperience of System Engineer assisting in the draindown. *-Human Engineering*	Human Engineering: -2; +1
6. Manual calculations required correction for nitrogen pressure effects.			6. Difficulty in local reading of tygon tube - poor lighting, etc. *-Human Engineering*	Supervision: -1; +1
7. Evening shift - 11:10 pm at time of RHR loss.			7. Entry into EOP delayed due to ambiguity in the entry conditions. *-Procedures*	Stress:
8. Plant behavior with respect to the "burping" action of the S/G tubes was different compared to previous draindowns. Past experience of one RO was that draining was almost done when burping stopped; could not tell when burping stopped during this draindown.				Design:

Source: AEOD Human Performance Study Report, April 1992.

through C.15. Two of these events, Prairie Island and Oconee, are the same as those reviewed in the AIT reports.

These five events include two losses of shutdown cooling, two losses of RCS pressure control (one over pressure and one underpressure), and one RCS LOCA. All were initiated by human errors, with two events having pre-existing latent failures caused by human errors. In each case, human actions taken in the control room recovered the plant; the times for recovery ranged from less than two minutes to 65 minutes.

Of the seven errors total (identified in the five events), four were errors of omission and three were errors of commission; of the errors of omission, most were performed by maintenance technicians. Control room personnel were principally involved with the errors of commission. Most of the errors were of the mistakes category involving actions in response to inadequately planned procedures or inadequate instrumentation.

C.2.4.4.2 Evaluation of Influences

Tables C.11 through C.15 identify the human errors, actions, and influences for each of the five events while Table C.4 summarizes the overall set of influences identified in all five event analyses.

As shown in Table C.4, the most significant negative influence was procedures (-10) specifically, providing insufficient information or not providing guidance in situations encountered. In each of the five events, procedures played a significant contributing role. Procedures more frequently were a negative contributor in initiating events then in event response (-6 versus -4). However, procedures were also one of the two most positive influences (+3) (e.g., providing adequate recovery guidance).

The second most important negative influence was organizational factors (-7); in four of the five events, organizational factors were indicated as contributing negatively to the event. In one case, coordination of activities at the organizational level did not exist such that incompatible activities occurred at the same time (i.e., performing multiple tests at

Braidwood Unit 1). In another case, a combination of a scheduling error and the lack of tags and/or formal control room records led operators to be unaware of the fact that key instrumentation was inoperable.

Communications (-6,+1) and human engineering (-6,+2) also played a significant role in these events. Communications were identified as a negative influence in all five events while human engineering was identified in three of the five events as a negative influence. Most frequently, the human engineering deficiencies were associated with poor or unreadable instrumentation (e.g., temporary level instrumentation) or inadequate labeling of components. Communica-tions problems were associated with failures to keep supervisory staff informed of changes in the plant, inadequate shift changeovers, or misunderstandings between the control room and other plant operators as to the coordination of activities.

Stress was identified as a contributing factor in the Crystal River Unit 3 and Braidwood Unit 1 AEOD reports. In both cases, the origin of stress was related to time - either time available for human actions, time of day (i.e., 3-4 am), or number of hours worked (i.e., 17 and 19 hours). As Table C.4 shows, the AEOD reports are the only event-based data source which record stress as a contributing influence.

A comparison of Tables C.13 and C.15 to Tables C.9 and C.10, respectively, shows that the human influence contributions identified in the AEOD reports for the Oconee Unit 3 and Prairie Island Unit 2 events were similar but not identical to those found in the parallel AIT reports. These differences may be attributable to the differences of focus for the two on-site investigations; i.e., human performance issues only for the AEOD reports and more general issues for the AIT reports.

Like the AIT reports, the AEOD reports contained information indicating the existence of both negative and positive attributes of influences impacting human performance. Examples of such attributes shown in Tables C.11 through C.15 are:

Procedures:

- *ambiguous entry conditions* delayed entry into EOP (Prairie Island)

- operators *did not use procedures in response* but instead used recall of procedures and plant behavior (Crystal River Unit 3)

- performance of two surveillance test procedures simultaneously allowed but *no formal procedure* for doing so (Braidwood Unit 1)

Training:

- operators *not trained on using draindown procedure* (mid-loop training not available on simulator (Prairie Island)

- operators *did not use an accepted rule of systems monitoring* - looking at all affected systems when a significant change in operating conditions occurs (Catawba Unit 1)

Communications:

- *insufficient information transferred during shift turnover/briefing* resulted in supervisors not being aware that two procedures were going to be performed together (Braidwood Unit 1)

- *shift briefing did not discuss* the significance of continued venting

Organizational Factors:

- using the flow diagram and note handwritten on the wall to locate penetrations was *contrary to site policy requirements* (Oconee Unit 3)

- decision to perform two procedures simultaneously made by two technical

staff engineering personnel (Braidwood Unit 1)

- *scheduling error left* three RCS pressure *instruments inoperable* and *no tags or formal log in CR for inoperable instruments* (Catawba Unit 1)

Supervision:

- inexperienced draindown crew *received infrequent supervision* by Shift Manager and Shift Supervisor because they were assumed to be experienced enough to proceed with draindown procedure (Prairie Island Unit 2)

- CR supervisors *not monitoring activities in CR* (Braidwood Unit 1)

Stress:

- significant actions took place between 3 and 4 am (when human performance is typically at its lowest) (Crystal River Unit 3)

- the two technical staff engineers performing test *had been working 17 and 19 hours*, respectively (Braidwood Unit 1)

C.2.4.4.3 Summary of Results

This study's evaluation of the AEOD reports are similar to that of the AIT reports and full-text LER evaluations in that: (1) all types of human errors and actions (i.e., initiators, pre-accident errors, and recovery actions) were identified; (2) procedures, training, communications, organizational factors, and human engineering influences were also identified as important contributors, and (3) multiple influences were identified. The information available in the AEOD reports also allowed the identification of influences which contributed positively to events and of attributes of influences which caused either positive or negative impacts on human actions or errors.

C.2.4.5 NUREG-1449, Shutdown and Low-Power Operations at Commercial Nuclear Power Plants in the U.S.

As summarized in Table C.4, the NRC staff discussed several human reliability influences in their draft NUREG-1449 evaluation of safety during LP&S operations. The sections most directly relevant to this project are Section 6.2, Outage Planning and Control; Section 6.3, Stress on Personnel and Programs; and Section 6.4, Training. Discussions of procedural and human-engineering issues are contained in the section specifically addressing loss of RHR capability, Section 6.6.1.

In Section 6.2, the NRC concluded that:

(1) consistent industry-wide safety criteria for LP&S operations do not exist;

(2) many licensees have no written safety policies providing LP&S safety operating criteria;

(3) some licensees enter planned outages with incomplete outage plans;

(4) some licensees cannot respond properly to an unscheduled outage because of poor planning;

(5) safety considerations are not always evident during outage planning;

(6) changes in outage plans and ad-hoc strategies often are not addressed as carefully as the original plan;

(7) the need for procedures and training is not always well addressed in planning;

(8) bases do not exist that establish fully an understanding of plant behavior and that would substantiate the techniques depended on to respond to events; and

(9) there is no regulation, regulatory basis, staff policy, or other guidance that requires or provides regulatory guidance

for outage planning or implementation of such planning.

In Section 6.3 of draft NUREG-1449, the NRC staff recognized that outage activities can stress the capabilities of plant personnel and the programs designed to ensure appropriate controls of safety and quality. Such stress can be reduced by ensuring that staffing levels for the outage are adequate, that appropriate training is provided, and that contingency plans exist for mitigating events during shutdowns. The staff noted that working hours of plant personnel were sometimes scheduled in ways incompatible with NRC's policy on work hours. The staff concluded, however, that the NUMARC Guidelines provide a sound approach addressing the issue of stress and its influence on risk (see Section C.2.4.6).

Training is discussed in Section 6.4 of draft NUREG-1449, specifically in regard to examination of reactor operators and the use of simulators in training. The staff recognizes that the current requirements for training has minimal compulsory coverage for LP&S operations, though these operations are included. The staff believes that, through improvements in outage planning, more training for LP&S operations will be addressed. Regarding simulators, their scope, based on ANSI/ANS-3.5-1985, does include normal control room operations from cold shutdown through full power and back to cold shutdown, excluding operations with the vessel head removed. However, ex-control room operations may be best addressed through other teaching methods. As the scope of LP&S training increases as a result of more comprehensive planning, the staff believes that the simulators will be used more frequently in LP&S training.

Issues associated with procedures and instrumentation during loss of RHR events in PWRs are discussed in Section 6.6.1 of draft NUREG-1449. Regarding procedures, the staff's principal concern is that alternative means of cooling the core following loss of RHR may not be soundly based. Human factors concerns associated with procedures are not discussed. The section on instrumentation briefly discusses the problems associated with the

measurement and display of RCS inventory level. In particular, the staff observes that operators are often unaware that core temperature cannot be inferred from RHR loop measurements when RHR is not operating, and that RCS water level indications continue to be a problem despite the issuance of NRC Generic Letter 88-17.

C.2.4.6 NUMARC 91-06, Guidelines for Industry Actions to Assess Shutdown Management

This industry document provides guidance to utilities in how to prepare for specific hazard states in planning for and controlling an outage. Specific hazard states addressed include loss of shutdown cooling, loss of inventory, loss of electrical supplies, and inadvertent reactivity addition. For example, the document discusses the key safety functions and alternative means of restoring them. The planning and control section, Section 3, discusses human factors issues, planning, and so on.

As Table C.4 shows, NUMARC provides guidance in several areas of interest to this project. Procedures are discussed in Section 3.3 - Providing Defense in-depth, and Section 3.4 - Contingency Planning. NUMARC recommends that "Procedures should be developed that are designed to mitigate the loss of KEY SAFETY FUNCTIONS." As part of contingency planning, procedures are one means of re-establishing the planned defense in-depth as equipment failures and human errors erode the defenses.

Training is identified specifically as a separate topic in Section 3.5 - Training. The NUMARC guidelines state that operator training should provide: (1) knowledge (through simulator training if practicable) of applicable safety issues associated with the expected outage, and (2) training for other plant personnel (including contractors and other temporary workers) for their assigned roles in outage activities that contribute to safety.

Organizational factors are discussed in Section 3.1, Integrated Management, and Section 3.3, Providing Defense in-depth. Section 3.1 indicates that senior management should issue a policy defining the nuclear safety philosophy for the outage, that schedules should be developed to ensure adequate defense in-depth and that changes in schedule should be reviewed for adequate safety coverage, that availability of key safety equipment and the performance of "higher risk evolutions" should be communicated frequently to personnel, and that post-outage critiques should be conducted to improve future performance. Section 3.3 of NUMARC 91-06 provides guidelines for ensuring an adequate depth of defenses. These include: using the outage schedule to establish which systems, structures and components provide safety function back-ups; optimizing the availability of safety systems; assuring the functionality of safety systems by means of testing and administrative controls; and developing appropriate procedures for mitigation of safety system losses.

Supervision is discussed in Section 3.6, Outage Safety Review. Guidelines in this area suggest: that the outage schedule should be reviewed by personnel not involved in its development to ensure that the management philosophy on outage safety has been implemented; that higher risk evolutions should be clearly identified and contingency plans exist; and that changes to the plan reviewed by appropriate levels of authority.

Finally, in Section 3.2, Level of Activities, the NUMARC guidelines recommend that an outage overtime policy should be established which requires prior approval by appropriate levels of management for overtime hours for outage personnel.

C.2.5 Conclusions Based on Data Analysis Review

First of all, the event analyses of the six data sources addressed during this study (i.e., NRC's draft NUREG-1449, NUMARC 91-06, NSAC-156, the four NRC AIT reports, the five NRC/AEOD human factors reports, and LERs) yield consistent results. The analyses based on the LERs (both in the present review and that of NSAC) provided an extensive survey of the types of actions involved during LP&S, the context in which actions and errors occur, and the "primary" influences affecting

the personnel. In this sense, "primary" influences are the immediate and direct influences that shaped the behaviors at the time the errors occurred. Particularly, there is a consistent pattern of procedures providing inadequate guidance or not covering actual situations, and inadequate human engineering such as poor instrumentation or inadequate labeling. As summarized in Table C.4, these two influences predominate in the evaluations based on LERs. In many cases, these human reliability influences resulted from temporary procedures, temporary or newly changed level instruments, and labels associated with equipment only operated or accessed during outages (as with the penetration labeling at Oconee Unit 3).

However, a more complex picture emerges following the review of the more detailed event analyses provided by the AIT reports and the human factors reviews for AEOD. In these studies, the same "influences" are still important but additional influences emerge to make the events more complex. In particular, training, communications, and organizational factors become apparent. What these "secondary influences" appear to indicate is that those plants that do not prepare comprehensively for LP&S operations may face unanticipated situations, for which no contingency plans exist, which are outside the envelope of the instrumentation, and for which no channels of communication are prepared. As seen in the patterns of multiple influences in Tables C.7 through C.15, a detailed examination of the events identified multiple influences (for example, see Table C.3), which usually act in a synergistic manner, thereby achieving an effect of which each individual contributing influence is incapable. In many cases, these multiple influences are the result of some common organizational deficiency such as inadequate identification of safety-critical plant evolutions. Perhaps the most glaring example was the loss of RHR at Prairie Island Unit 2, on February 20, 1992 (Tables C.10 and C.15). This event was the result of performing a reduction in RCS level at a time when decay heat was significant. The procedure for level control involved detailed and extensive manual calculations to convert measurements taken at the poorly cited temporary RCS level instrumentation, but the

experienced personnel were not performing the task. No job aids or training were provided, and no supervision in the control room was provided to help manage the evolution. All these influences can be seen as arising from a lack of management awareness that this evolution was inherently risky, since no compensating measures were taken and it occurred when the decay heat level was significant.

In terms of the kinds of errors, the inevitable consequence of combinations of influences, such as those identified in the AIT and AEOD reports, is that mistakes will be induced by the lack of adequate procedures and instrumentation. These mistakes will be principally rule-based (use of inadequately planned procedures and inadequate knowledge of the plant state). Because so many tasks involve direct manual interactions, the result is often errors of commission--namely, operators take the wrong actions or take an action at the wrong time. This result is in contrast to full-power operations where operators are more frequently performing a supervisory function of monitoring automatic equipment.

The LER-based data provided little information on the recovery of events (other than the timescales) for human and hardware responses; whereas the more detailed analyses indicate that, in most cases, procedures and training were effective in ensuring an adequate recovery. In fact, the apparent paradox of the same influences scoring both positive and negative in Table C.4 is because the "temporary" procedures or training were a significant causal factor in creating the event, but the "permanent" procedures and training resulted in recovery of the event. Only those events involving mechanical damage and short timescales for core heatup were problematic.

C.3   Interviews with Knowledgeable Individuals

C.3.1   Interview Protocol Development

To complement the classification of data extracted from LP&S reported events and associated studies, interviews were held with knowledgeable NRC, Industry (EPRI and NUMARC) and utility personnel. A standard interview protocol consisting of questions pertaining to LP&S issues was developed for this purpose.

The interview protocol provided the interviewers with a standardized means for obtaining interviewee responses on LP&S issues including: important lessons to be learned from reviews of LP&S activities; important characteristics of LP&S operations that influence safety; important LP&S human reliability influences; differences in human influences between LP&S and full power operations; and important observable factors that distinguish a good outage from a poor outage. Additional questions solicited insights an interviewee might have gained through exposure to LP&S incidents with significant human performance implications. To accommodate differences in operational information, a slightly revised protocol was utilized for interviews with utility personnel. The results of interviewee responses to each of these LP&S issues are discussed in Section C.3.3. Section C.3.3.1 discusses the results from interviews with NRC and industry personnel, while Section C.3.3.2 discusses the results from utility personnel.

C.3.2   Interviewee Experience

Interviewees were selected to provide a diversified representation of knowledgeable individuals in the areas of human performance and LP&S operation. This sample included NRC, EPRI, NUMARC, and utility personnel. Interviewees were involved with LP&S-related reports and guidelines, data source development, plant visits (i.e., AITs, IITs, and EOP inspections), the accident sequence precursor program (analysis of LP&S events), and LP&S plant operation, including maintenance, training, and planning.

C.3.3   Results of Interviews

C.3.3.1   Information Obtained from Interviews with NRC and Industry Representatives

C.3.3.1.1   Challenges to Plant Safety Associated with LP&S

Plant configuration when an event occurs was reported to have a significant impact on event severity and mitigation. An example provided by one interviewee was the Diablo Canyon Unit 2 incident of April 10, 1987, which involved the loss of reactor heat removal. An analysis showed that since the primary system was not open, the operators easily handled the event with no serious consequences. On the other hand, had the event occurred a half an hour earlier (when the steam generator primary manway was off), the core would have been uncovered in a short time.

Movement of radioactive fuel was reported to impact safety. Examples of fuel being shuffled into locations which had been unanalyzed and into loadings where instrumentation did not provide meaningful indications of approaching criticality were cited.

Other plant configuration characteristics reported to impact safety included the ability to close containment, reduced RCS inventory control, decay heat removal, and less than adequate control over switchyard activities.

C.3.3.1.2   Performance Influences Unique to LP&S

It was reported that during shutdown plant configurations are changing continuously and human-system interactions are much more frequent.

There are major configuration changes, more people, and an increase in diverse activities making control and communication a more demanding task. The overall consensus was that LP&S was a more complicated and dynamic condition requiring a different approach than that of normal operation, with a much greater emphasis on the importance of communication, organizational factors, supervision, and stress.

Procedures and training were rated high in importance and applicable to both initiators and recovery of LP&S as well as full-power events. A synergistic relationship was reported to exist between procedures and training such that if both were "bad," the operators could really get into trouble. However, good training could compensate for inadequate procedures.

Stress, communication, human engineering, supervision, and organizational factors were reported to be situation-specific with respect to their importance as potential contributors to human performance during LP&S. Stress due to fatigue was reported to be more important as an influence for plant staff than for contractor staff and was considered an important influence to both event initiation and recovery, especially when coming out of an outage. Communication was discovered to be an important influence for both event initiation and recovery, especially during equipment configuration changes. Human engineering and supervision were rated low in importance as recovery influences but high as influences to event initiation. In general, supervision and organizational factors were rated lower in importance while at full power than during LP&S.

C.3.3.1.3   Maintaining Plant Safety During LP&S

Training was reported to be of significant importance for maintaining plant safety during LP&S. It was stressed that with adequate training operators would not be surprised, or ill prepared, when unexpected or unanalyzed phenomena occur. It was further stressed that communication played a significant role, especially with respect to communicating experience from past events and

PRA findings to improve the knowledge base of working level personnel. The importance of having systems beyond instrumentation (e.g., outage control centers to communicate timely and reliable indications of plant status and configuration to plant personnel was cited.

Additional reported issues included the importance of addressing changes in work assignments (roles and responsibilities) and the need to control and coordinate group activities. An example provided made reference to the very different role the control room crew has during LP&S and the influence these role changes have on performance. In addition, the vast increase in work activities being performed on multiple components makes control and coordination of LP&S activities a critical concern.

The process of entering or exiting an outage was reported to create an environment conducive to errors. Keeping communication lines open during such major transitions (which could be prolonged over several shifts) and minimizing time lag of information dissemination were reported to be of paramount importance. Another recommendation provided was to use the same people each outage to make use of accumulated experience.

Poor outage planning was cited as being a significant contributor to many LP&S events. It was recommended that outage planning should focus on safety functions and not solely on desired equipment maintenance.

It was further recommended that the licensee's outage plan be clearly understood. Planning procedures should be available and utilized. The plan should make schedule sense (i.e., is equipment available when needed the most) and address safety reviews, ways to prevent failures, feedback mechanisms as well as allocation and control of resources. It should contain an identification of the vulnerabilities (i.e., the critical functions that must be maintained) and specifications for contingency plans. The plan should also include a reasonable assessment of resources in terms of people and hours per task, and a clear program to ensure coordination and communication between all groups (e.g., end of shift meetings). The plan should not

contain any unfamiliar task or configuration requirements.

Other important factors identified as being important for maintaining plant safety during LP&S include provisions for defense in-depth, adequate training, a safety attitude (culture), sufficient levels of supervision, and barriers and notices protecting critical equipment.

Several interviewees commented on the need for additional requirements (e.g., technical specifications) to control shutdown conditions. European plants were cited as taking a much more cautious view of plant risk during LP&S and having more stringent technical specifications covering LP&S plant configurations.

C.3.3.2 Information Obtained from Interviews with Utility Personnel

C.3.3.2.1 Challenges to Plant Safety Associated with LP&S

The greatest challenge to critical safety functions comes from the possibility of simultaneous unavailability of equipment causing the loss of a given function. There was general agreement that operating with reduced RCS inventory under circumstances in which the RHR function might be compromised represented a serious challenge to the safety of the unit.

C.3.3.2.2 Performance Influences Unique to LP&S

During an outage, the role of the operations staff changes considerably as compared with full power operation. Full power operations were characterized as more relaxed, consisting of such activities as surveillance testing, review of procedures and training. The operator responsible for the "up" unit of a two-unit plant during an outage has the added task of closely monitoring activities in the "down" unit, since there may be common equipment or cross-tie capability. The operating circumstances during an outage are more demanding, the work more intensive, and shift turnovers more difficult. Reduced inventory operations were identified as

presenting the greatest challenge to the operator. Also noted as difficult were maintaining awareness of plant status, keeping track of unavailable equipment, and avoiding loss of information during shift turnovers.

From the operators' perspective, the level of concentration required of the operators is the primary difference between at-power and LP&S operations. There are more people working in the control room and an increased number of manual interventions and manipulations needed in LP&S.

The number and complexity of the maintenance activities performed during LP&S operations is greatly increased. The tasks are also typically longer in duration than during full power operations, so that communication during shift turnovers becomes an important factor.

C.3.3.2.3 Maintaining Plant Safety During LP&S

Utility personnel reported that critical safety functions are protected by proposed outage activities being subject to multiple reviews. The operations manager and operations coordinator review plant technical specifications, outage activities and "windows" (i.e., periods of time during which activities may occur). Proposed outage activities are also reviewed by the shift supervisor. The SRO in the control room is ultimately responsible for any activity performed on his shift, although ROs will also be familiar with technical specifications and other requirements.

As noted above, PWR reduced inventory operations (i.e., midloop) are the most challenging conditions. In addition to the above reviews, safety is maintained during reduced inventory operations by the presence of two independent RCS level indications in the control room (in addition to local sight glass indication used during draindown). Procedures call for results of mass balance calculations to be constantly compared to level indications.

Operators are periodically trained in RHR operation; such training is scheduled as close to the start of an outage as possible. Specific pre-outage training and

operational checks are designed to avoid entering adverse configurations. Training is provided on the RHR system, draindown and midloop. Loss of RHR accidents and mitigation are simulated. These topics are refreshed in requalification training. An attempt is made to present such simulations just prior to an outage if possible. In the opinion of some interviewees, RCS draindown is not particularly troublesome at present since procedures and training have been optimized based on industry experience with LP&S.

Staffing changes reflect changes in the difficulty of the operator's role such that additional RO and SRO personnel are assigned to the "down" unit during an outage. As many as five SROs may be on a shift during an outage. In addition, paperwork related to work orders, tagouts, etc. is handled outside the control room during an outage in order to reduce the load on control room operators.

Interviewees were in agreement that outage planning was important to the success of the outage. Maintenance personnel judged the availability of manpower and replacement parts to be critical to safe and timely completion of outage maintenance. Coordination and communication with operations personnel were also seen as important. Outage planning personnel emphasized that the success of an outage depends on close, continuing coordination with operations personnel and meticulous management of the plan as it evolves through multiple revisions. Outage planners further remarked that they made a concerted effort to involve personnel from all functional groups (operations, maintenance, engineering, management) in the development of the outage plan. It had been their experience that participation leads to commitment and a willingness to take responsibility, while lack of involvement leads to resistance and fault-finding.

C.3.4   Conclusions Based on Interviews

Utility personnel provided the insight that operating with reduced inventory under circumstances in which the RHR function might be compromised posed a very real concern about plant safety. NRC and industry personnel echoed these concerns and specified fuel movement, containment closure, and switchyard control as additional challenges to plant safety during LP&S operation.

Similar insights were reported on the differences between LP&S and full power human reliability influences. Both groups cited changing roles for plant personnel, increased work activities, and the critical importance of communicating plant status as significant human reliability influences unique to LP&S. Utility personnel elaborated on these differences emphasizing shift turnover and the increased number of manual (human) interventions and manipulations required during LP&S, while NRC and industry personnel emphasized the increased importance of training and procedures.

Utility personnel insights on maintaining plant safety during LP&S had an expected plant operations emphasis (i.e., specific examples of necessary instrumentation and RCS drain down training were provided). Utility planners highlighted the importance of involving personnel from all functional groups in the development of the outage plan. Both groups similarly reported on the critical role a well developed outage plan, coupled with adequate training, procedures and staffing, plays in maintaining plant safety. NRC and industry personnel provided insights on the particular problems represented by transitions such as entering and exiting an outage. The need for additional technical specifications to control LP&S activities was expressed by NRC personnel.

C.4 Results and Conclusions

This section presents the results of the evaluation of event and non-event data and the interviews with knowledgeable personnel. Section C.4.1 summarizes the results in terms of the kinds of errors and actions, the influences that bear upon these errors and actions, and how these may differ from full power operations. Section C.4.2 discusses these results in terms of their implications for the selection of frameworks and development of methods for detailed human reliability analyses of LP&S operations.

C.4.1 Results

The results of this work are: (1) a characterization of the human actions and errors that could have a significant impact on safety during LP&S operations; (2) an evaluation of primary influences on human performance during LP&S operations; and (3) a review of how these actions, errors, and influences differ from those human actions, errors, and influences important to safety during full-power operations.

C.4.1.1 Characterization of Human Actions and Errors During LP&S

There is a consistency in results between the evaluation of data described in Section C.2 and the opinions of knowledgeable individuals summarized in Section C.3. For example, operations during outages identified as important to safety in both the event analyses and the interviews were associated with lowering RCS water level, and maintaining electrical supplies were identified as important to safety in both the event analyses and the interviews. During these operations, configurations can be encountered that make the plant more vulnerable to errors by personnel or failures of equipment. Examples include the limited margins for error in level control during mid-loop operations, where vortexing may lead to loss of all RHR pumping. In particular, it is the unique combination of unusual plant vulnerabilities together with the increased

opportunities for errors during unusual evolutions that make LP&S operations of concern.

Because human-system interactions during LP&S operations are more direct, with operators more frequently manually operating equipment and changing plant configurations, there is a greater opportunity for these interventions to "go astray," resulting in mistakes leading to errors of commission. In many cases, these mistakes are the result of poorly developed procedures that fail to provide guidance in some part of an evolution, such as when the equipment does not operate as assumed in the procedure, or there is simultaneous work proceeding in another part of the system. This is reflected in the interview comments about the importance of outage planning and the need for LP&S-specific technical specifications.

Both latent and active errors appear to play a significant role. In most of the detailed event descriptions (i.e., AIT and AEOD report analyses), both latent and active failures were present to cause the situation; this was less clear in the LER-based information, however. In all three event-based data sources, active human error most likely initiated the event.

Recovery of failed safety functions was accomplished in all cases before plant damage occurred, usually through manual actions. A wide range of times until recovery was reported both in the LER and more detailed data. The longest times (> 4 hours) were often associated with situations where partial recovery of equipment occurred (as with venting of an RHR pump) only for the equipment to fail again (as when the cause of the pump air-binding was not corrected) before being finally restored. The shortest times (< 1 minute) involved simple switching actions in the control room such as reclosing a circuit breaker.

C.4.1.2 Evaluation of Primary Human Reliability Influences During LP&S

As with the kinds of errors and actions, there seems to be a convergence in the findings of important human reliability influences from the evaluation of events and from the interviews. Through all the sources of information, the most frequently identified influence is procedures. The event data indicate that procedures are frequently deficient, either in providing inadequate guidance or in omitting instructions for unexpected contingencies while performing evolutions. The interviews indicate procedures are rated highly as a human reliability influence, particularly in certain plant configurations when other influences come into play. These other situation-specific influences include human engineering, communications, organizational factors, and stress. This combination is again reflected in the interviews and the event data, especially the more detailed analyses of the AIT and AEOD reports. The combination of influences (as many as three or four) is seen as an important finding in this study.

One observation from the interviews was that the safety concerns and influences are very situation-specific. This was not directly observable from the event data but could be inferred from the number of reports associated with specific plant conditions, most noticeably lowering RCS water level in the transition to mid-loop operations. Another situation-specific concern was the period where limited electrical supplies (on-site or off-site) were available. Typically, single errors were sufficient to initiate significant safety challenges in those conditions. In addition, in the case of changing to mid-loop operations, the plant is in a dynamic state such that operators are more challenged in tracking parameters using (often inadequate) instrumentation and procedures.

Recovery actions were frequently aided by use of abnormal or other contingency procedures once an event had been initiated and (often) a safety function was lost. In addition, the detailed event analyses and the interviews indicated that training and the detailed technical knowledge of plant operators can be important in assisting in the recovery of lost safety functions and stabilization of the plant.

In summary, the principal findings in terms of influences on human performance are that:

- most events of any significance to safety involve multiple influences;

- the most frequently cited human reliability influences are procedures and human engineering;

- the more detailed descriptions of events indicate that these deficiencies are symptomatic of poor planning and preparation, as indicated by frequently concurrent deficiencies in training, communications, and organizational factors;

- the combinations of influences giving rise to performance problems appear to be very sensitive to the context of the plant conditions; and

- recovery is frequently aided by situation appropriate procedures, specific training, and the technical knowledge of the operations personnel.

C.4.1.3 Differences Between Full-Power and LP&S Operations

Through the data evaluations discussed in Section C.2 and the opinions of knowledgeable individuals given in Section C.3, a number of significant differences between the human actions, errors, and influences important to LP&S operations and that of full-power operations have been identified. Aspects of the following identified features are unique and important to LP&S operations: the kinds of human interactions and events; the classes, modes, and types of human errors (and actions); influences on human performance; and plant conditions and configurations.

Unlike full-power operations, all classes of human actions and errors (i.e., initiator, pre-accident, and recovery) seem to play a significant role in LP&S operations and events. In particular, human-initiated events typically are not explicitly treated in full-power PRAs. It is typically assumed that human-initiated events at full power are relatively uncommon and can be captured in data collected at the component, system, or plant level. For LP&S events, however, human-induced initiators, both inside and outside the control room, comprise a significant portion of observed errors. This phenomena may be the result of the more direct human-system interactions characteristic of LP&S operations (see discussion in Section C.4.1.1).

The data evaluations given in Section C.2 indicated that mistakes (vs. slips) and errors of commission (vs. omission) predominate the types and modes of human errors which occur during LP&S. In addition, mistakes and errors of commission occur both inside and outside the control room during LP&S. As discussed in Section C.4.1.1, the more direct human-system interactions characteristic of LP&S operations can result in mistakes which, in turn, lead to errors of commission. In contrast, the human errors modeled in full-power PRAs are typically errors of omission (for example, the NRC Generic Letter 88-20 does not require errors of commission to be modeled in licensee Individual Plant Examinations (IPEs)), and mistakes are predominately modeled as in-control room errors.

The data collection efforts of this endeavor have resulted in the identification of several important influences on human performance during LP&S. Both the event-based data sources and the interviews identified procedures, human engineering, training, organizational factors, and communications as significant contributors to human errors and actions.

The human errors modeled in full-power PRAs are typically errors of omission or mistakes are occurring inside the control room.

Procedures, human engineering, training, organizational factors, and communications were identified as significant influences on human performance during LP&S. Procedures are typically

important in modeling human errors in full-power PRAs. However, human engineering (especially in the control room), organizational factors, and communications, as well as the less important influences identified in Table C.4, are not typically identified as important influences on human performance at full power. In addition, the event-based data evaluations strongly indicated that contributions from multiple influences are common for human actions and errors during LP&S. Also, the available time for event response, frequently an important factor in human performance at full power, does not appear to be a concern. (An exception is likely to be made for events initiated shortly after shutdown when decay heat is high).

Unlike full-power operations, LP&S operations are performed under continuously changing plant conditions and configurations. Frequent changes in the plant situation result in changes in the potential consequences of events and the availability of redundant (and, in some cases, front-line) equipment in event responses. In addition, the changing plant environment during LP&S increases the importance of communications in order to safely perform outage activities and to appropriately respond to LP&S events. Also, as mentioned in Section C.4.1.1, equipment is more frequently manually operated during LP&S operations, and responses to LP&S events are also typically achieved through manual human actions rather than automatic equipment response.

C.4.1.4   Proposed Influences for Detailed HRA Quantification

Based on the evaluation of primary human reliability influences and the discussion of the differences between full-power and LP&S operations in Sections C.4.1.2 and C.4.1.3, respectively, the following influences are proposed for consideration during LP&S detailed HRA quantification:

- procedures
- training
- communication
- organizational factors
- human engineering

- supervision

Note that depending on the particular LP&S human action, two or more of the above influences may have to be used in various combinations.

C.4.2   Conclusions

The conclusions of this work are that human actions and errors are important contributors to risk during PWR LP&S operations. In particular, the principal errors that seem important under such conditions are associated with manual control actions (e.g., reducing level) and control of equipment configuration for maintenance and test that lead to loss of defense-in-depth. The quality of procedures and information systems (e.g., temporary instrumentation, number of alarms indicating, etc.), and control and coordination of plant status (e.g., inadvertently working on two trains) influence human performance and play an important role in the frequencies of errors in LP&S operations. Recovery actions seem to be available for most kinds of problems, though failures during the early stages of an outage when decay heat levels are still significant present greater challenges because of reduced timescales to core uncovery. These kinds of problems are different from those during full power operations in that a much greater emphasis is placed on manual control actions. Also, personnel not normally at the plant (e.g., headquarters engineering and contractors) and not intimately familiar with the day-to-day work practices and normal operating procedures may be performing tasks important to safety. In addition, real or perceived problems can exist in terms of the operators' ability to observe the state of the plant and the configuration of its equipment. These differences from full-power operations help create a situation where errors are more likely and their consequences less observable. A significant mitigating factor is that, after the first few days of an outage, the time required for fuel uncovery to occur following loss of cooling, for example, is sufficiently extended such that delays in recovering from errors can be tolerated with less impact on risk.

It should be recognized that the methods used by plants to plan for, and control, outages have changed and will continue to change. For example, plants are now completing their responses to NRC's generic letter issued in 1988 following the Diablo Canyon event. In addition, the NUMARC 91-06 guidelines, issued in December 1991, are intended to improve the planning and management of outages, particularly in preparing defenses for inadvertent accidents. Therefore, it is recognized that some of the issues described in this report may become less significant. However, as the Prairie Island Unit 2 event in February 1992 shows, plants continue to demonstrate vulnerabilities in LP&S operations.

These conclusions set the stage for the development of human reliability methods in the next phase of the project. The following are considered the most important factors that will determine the selection of a framework and development of a method for quantifying human reliability parameters:

- errors important to safety, particularly those that initiate events, are very context-specific and therefore the framework will need to account for the context in which actions are taken - this context may require more information about dynamic plant conditions than a typical PRA cutset scenario provides;

- the kinds of errors, particularly mistake-driven acts of commission, that have been found to be very important in LP&S events are not considered in any of the commonly used human reliability methods - those methods evaluating acts of commission (e.g., THERP) do so only for slip-driven acts, not for mistake-driven ones;

- the synergistic effects of multiple influences, e.g., procedures, training, human engineering, etc., are not practically considered in any commonly used human reliability methods, nor are the implications of inadequate planning and control of an outage;

- the presence of a much larger and less experienced body of staff at the plant, as well as the influence of extended work periods, can play significant roles in increasing the workload of operators. These sources of <u>stress</u> are not considered in any commonly used human reliability methods; and

- commonly used techniques used to model recovery actions do not take into account the possible complexities of <u>restoring mechanically failed or disassembled equipment</u>.

NUREG/CR-6093

C.5 References

AEOD Human Factors Team Report - Catawba, Unit 1 - March 20, 1990, "On-Site Analysis of the Human Factors of an Event," U.S. Nuclear Regulatory Commission, May 1990.

AEOD Human Factors Team Report - Braidwood, Unit 1 - October 4, 1990, "On-Site Investigation and Analysis of the Human Factors of an Event," U.S. Nuclear Regulatory Commission, October 1990.

AEOD Human Performance Study Report - Oconee, Unit 3 - March 8, 1991, "On-Site Analysis of the Human Factors of an Event (Loss of Shutdown Cooling)," U.S. Nuclear Regulatory Commission, May 1991.

AEOD Human Performance Study Report - 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, January 1992.

AEOD Human Performance Study Report - Prairie Island, Unit 2 - February 20, 1992, "On-Site Analysis of the Human Factors of an Event (Loss of Shutdown Cooling)," U.S. Nuclear Regulatory Commission, March 1992.

AEOD Special Evaluation Report, "Review of Operating Events Occurring During Hot and Cold Shutdown and Refueling," U.S. Nuclear Regulatory Commission, December 4, 1990.

Generic Letter No. 88-17, "Loss of Decay Heat Removal," U.S. Nuclear Regulatory Commission, October 1988.

Generic Letter No. 88-20, "Individual Plant Examination," U.S. Nuclear Regulatory Commission, November 1988.

Inspection Report No. 50-306/92-005, Prairie Island, Unit 2, "Loss of RHR (February 20, 1992),"

Augmented Inspection Team Report, U.S. Nuclear Regulatory Commission, March 17, 1992.

Inspection Report No. 50-275/91-009, Diablo Canyon, Unit 1, "Loss of Off-Site Power (March 7, 1991)," Augmented Inspection Team Report, U.S. Nuclear Regulatory Commission, April 17, 1991.

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

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

NSAC-52, "Residual Heat Removal Experience and Safety Analysis, PWRs," Electric Power Research Institute, January 1983.

NSAC-84, "Zion Nuclear Power Plant Residual Heat Removal PRA," Electric Power Research Institute, January 1985.

NSAC-156, "Residual Heat Removal Experience Review and Safety Analysis, PWRs, 1982-1989," Electric Power Research Institute, August 1991.

NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management," NUMARC, December 1991.

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

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, June 1990.

NUREG-1449, "Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States," Draft Report for Comment, U.S. Nuclear Regulatory Commission, February 1992.

NUREG/CR-3905, "Sequence Coding and Search System for Licensee Event Reports," U.S. Nuclear Regulatory Commission, April 1985.

NUREG/CR-4639, "Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), User's Guide Volume 4," U.S. Nuclear Regulatory Commission, October 1990.

NUREG/CR-5655, "Human Performance Investigation Process (HPIP)," U.S. Nuclear Regulatory Commission, 1991.

Reason, James, Human Error, Cambridge University Press, 1990.

Senders, John W., and Moray, Neville P., Human Error: Case, Prediction, and Reduction, Lawrence Erlbaum Associates, 1991.

APPENDIX D

IMPROVED PRA PROGRAM PLAN

OUTLINE

Draft Letter Report

Proposed by

Brookhaven National Laboratory (BNL) and Sandia National Laboratories (SNL)

(Under NRC/RES FINs L2415 {BNL} and L2439 {SNL}

W. Luckas, BNL
J. Wreathall, J. Wreathall & Co.
S. Cooper, SAIC
D. Bley, PLG, Inc.
W. Brown, BNL
M. Barriere, BNL

D. Whitehead, SNL
G. Parry, Halliburton NUS
P. Haas, Concord Associates Inc.
M. Donovan, Halliburton NUS
J. Forester, SAIC

Table of Contents

Figures

Tables

D.1. Introduction

Human reliability analysis (HRA) is an integral part of probabilistic risk assessments (PRAs). Although various approaches and methods have been proposed since the first HRA was performed as part of the Reactor Safety Study, WASH-1400 almost two decades ago, the technology associated with HRA is still not fully developed. Additionally, recent studies and events indicate that the dominant sources of plant risk in low power and shutdown (LP&S) operations are frequently either human-induced initiators or errors of commission. Presently, there are no HRA methods or techniques that account for these types of human actions or explicitly enable their integration into the PRA. Development of new or improvements in existing HRA methodologies must be achieved in order increase the robustness of PRAs for all modes of plant operation and to specifically support the performance of LP&S PRAs.

1.1 Background

Better integration of the HRA into the PRA process has been a recognized concern for some time. For instance, the review of the NUREG-1150 PRAs, particularly the comments by the Kouts Committee (NUREG-1150, Vol. 3, Appendix E.5.1), pointed out various deficiencies in the human reliability analysis performed in these most recent NRC-sponsored PRAs. In its response to these review comments, the NRC states that "the demonstration and more widespread use of improved HRA methods in PRA is planned to be the subject of future work by NRC."

With respect to evaluating the risks associated with plant activities during shutdowns, the NRC's Office of Nuclear Regulatory Research (RES) initiated its LP&S PRA program during Fiscal Year 1989 as a result of the Chernobyl accident and other precursor events (e.g., Diablo Canyon). Shortly after the LP&S program was initiated, an event at the Vogtle plant (March 1990) occurred and, more recently, an event at the Prairie Island plant (February 1992), highlighting the importance of the RES program to examine the potential risk during LP&S operations.

Evaluations of events which have occurred during shutdown, such as NUREG-1449 and NSAC-52, have indicated that human activities and performance play a much larger role in shutdown than during full power operations. At many plants, all or most automatic safety functions and alarms are disabled, few technical specifications apply, and configuration-specific emergency procedures are unavailable. During the shutdown process, operators continually change the reactor coolant system-related configuration to accommodate process requirements. Configuration changes often involve reduced inventory or solid water conditions. It is also necessary for safety and support equipment to be taken out of service for maintenance in coordinated fashion.

As part of NRC's LP&S Program in 1992, a detailed examination of the role of human activities during shutdown was performed. Parallel efforts for the pressurized water reactor (PWR) and boiling water reactor (BWR) were performed, involving interviews of knowledgeable personnel (e.g., NRC staff, industry representatives, Grand Gulf and Surry staff) and the collection and evaluation of LP&S-related reports and event data (e.g., Licensee Event Reports (LERs) and Augmented Inspection Team (AIT) reports.) Together, Brookhaven National Laboratory (BNL) and Sandia National Laboratories (SNL) developed the "Human Action Classification Scheme (HACS) for BWR and PWR Low Power and Shutdown Plant Operational States" which was used to build separate PWR and BWR data bases containing event-based, LP&S data and analysis results. The PWR and BWR studies identified classes of human errors and human reliability influences which are unique to LP&S and developed a classification scheme for the types or classes of human errors that occur. For example, the draft BNL report on PWRs identified important conclusions regarding unique features of LP&S events and deficiencies in full-power PRAs such as:

1. Certain kinds of errors have been found to be very important in LP&S events, in particular mistake-driven acts of

commission (i.e., errors of commission). However, these errors are not considered in any of the commonly used human reliability methods; those methods which evaluate acts of commission (e.g., THERP) are applicable only to slip-driven acts, not to mistaken-driven acts.

2. Multiple influences were found to contribute to human reliability and performance in many LP&S events. However, the synergistic effects of multiple influences are not practically considered in any commonly used human reliability methods. Also not addressed in HRA methods are the implications of inadequate outage planning and control which appeared to be important causes of human errors in many LP&S events.

3. Many LP&S events were initiated by human errors. In full-power PRAs, human-induced initiators are typically assumed to be relatively infrequent and, therefore, are not explicitly treated in PRAs. Such initiators are not commonly treated by human reliability analysis methods.

4. Several LP&S events were identified as involving dependencies between human errors of different classes (e.g., pre-accident errors, initiators, post-accident errors). Dependencies between human errors are not commonly treated in PRAs.

5. Unlike full-power operations, LP&S operations are performed under continuously changing plant conditions and configurations. As a result the number of human activities which occur during shutdown is much greater than that at full-power. LER evaluations showed that there is a potential for unanticipated interrelationships between these various tasks, which do not necessarily involve human errors. Such interrelationships are not addressed in current PRAs.

The draft SNL report on BWRs identified parallel and complementary results. For example, approximations from the BWR LER data reviews indicated the following frequencies for human-induced initiating events:

- Loss of shutdown cooling: 0.98 events/calendar year, 3.28 events/shutdown year

- Loss of reactor coolant inventory: 0.24 events/calendar year, 0.82 events/shutdown year

- Loss of electrical power: 0.57 events/calendar year, 1.91 events/shutdown year

- Inadvertent engineered safeguards features actuation: 2.47 events/calendar year, 8.25 events/shutdown year

1.2 Objectives and Scope

The overall program objective is to develop a substantially improved quantitative human performance modeling process; i.e., a method for evaluating the risk impact of human interactions with nuclear power plant systems. Improvements are demanded in cognitive modeling, tracking influences from both the human and the plant PRA models, and ensuring that the PRA model, representing the plant and its personnel, can computationally replicate the identifiable influences.

The specific program objectives are:

a. Provide improved guidance (i.e., beyond NUREG-1150) for computationally incorporating the improved human performance modeling process into PRA,

b. Report on the insights pertinent to human reliability concerns which were gained in the evaluation of LP&S events,

c. Develop improved methodologies and methods for LP&S-specific human

reliability concerns such as human initiators, errors of commission, and dependencies, and

d. Develop a generic implementation guidance document which address, for example, LP&S-specific human reliability concerns.

This document, the IMPROVED PRA Program Plan Outline, delineates the specific products of the program, provides estimates of the required level of effort, and provides a schedule for completing the program. Figure 1 provides a flow diagram of the program plan tasks that will be described in detail in Section 2.

In order to provide input expeditiously to the NRC's LP&S Program, some tasks of the program plan will be performed in parallel. A report on LP&S evaluations will be issued three months after the start of the program while other development tasks are ongoing. HRA methodology development efforts and a draft of the implementation guidelines will be completed by the end of first year. The draft guidelines will be tested during a trial demonstration and revised as necessary by the end of the second year.

1.3 Regulatory Applications

In the short term, the IMPROVED PRA program will provide comprehensive HRA support to the LP&S Level I PWR and BWR PRAs. These PRAs are expected to support the NRC staff's regulatory analysis for a ruling on shutdown. The program will have developed the required methods and techniques for addressing LP&S-specific human failure events one year after the program is initiated.

Generally, products from the IMPROVED PRA program will provide improved PRA methods in the areas of:

- Improve guidance for incorporating HRA into PRA

- Improve representation of human failure events in event trees and fault trees (e.g., update of NUREG-1150 models)
- Evaluate significance of errors of commission
- Represent and evaluate dependent human failure events
- Represent and evaluate human-induced initiators
- Evaluate the potential for instrumentation unavailability and its impact

Potential application of the improved PRA methods include:

1. Methods to provide qualitative and quantitative assessments:

- Evaluate industry-proposed requirements and guidelines
- Evaluate outage planning and control
- Provide assistance in critical training needs identification
- Evaluate procedures used for shutdown accidents
- Provide input to potential accident management strategies

2. Development of operations and training improvements:

- Develop procedure (e.g., emergency, abnormal, operating, function restoration, and emergency contingency action)
- Develop simulator scenarios

3. Provide input to plant shutdown safety improvement:

- Provide input to industry-proposed guide-lines (i.e., NUMARC 91-06)
- Identify methods to reduce the frequency of accident initiators (especially those human-induced)
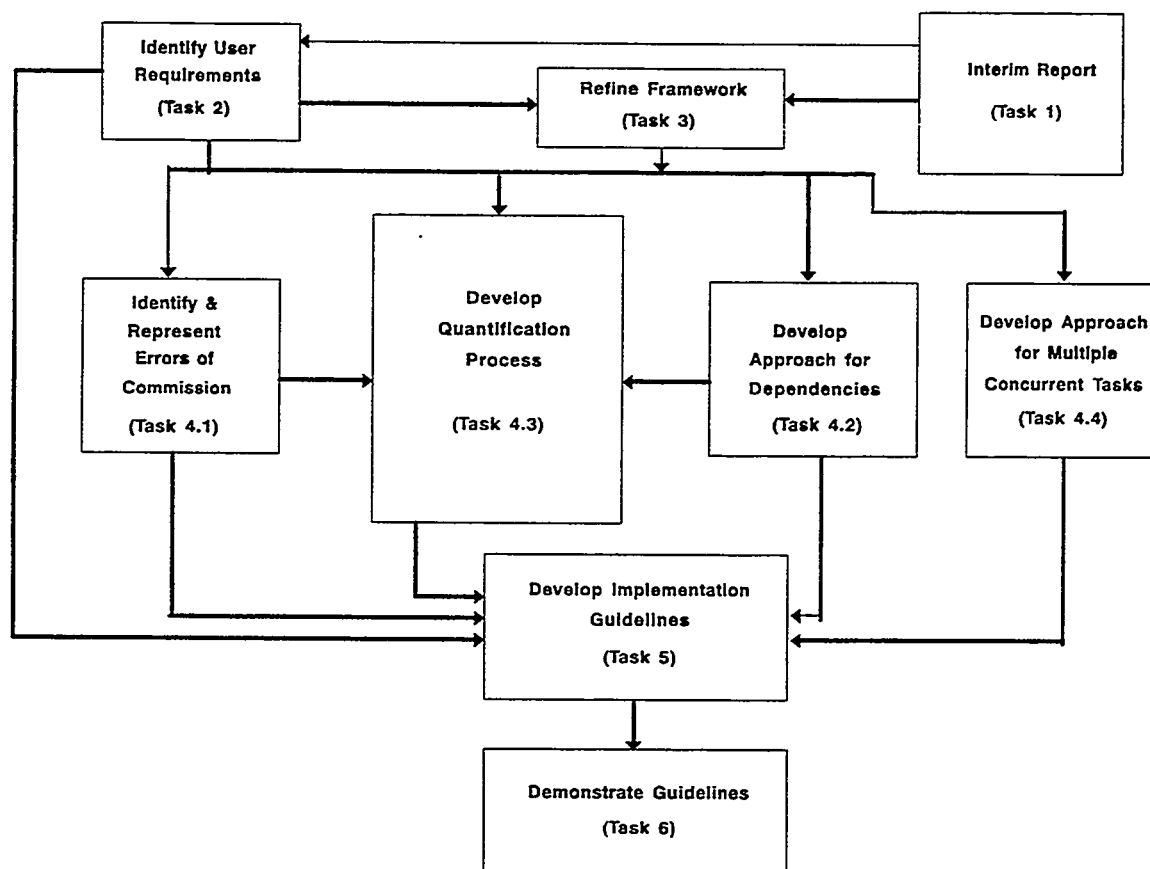- Identify important areas for shutdown inspections

Figure 1. IMPROVED PRA program plan tasks - flow diagram

2. Tasks and Products

2.1 Requirements for an Improved Human Performance Modeling Process

An improved human performance modeling process is necessary because the current state of knowledge (with respect to the ways operators and other personnel interact with the plant and impact its safety) has outstripped present modeling capabilities. The operators, in particular, are integral to maintaining plant safety. There are also circumstances when other personnel can significantly impact plant safety. For PRA results to be useful in risk management and risk-based regulation activities, they must replicate our best understanding of the human-machine combination. There are specific areas where current human modeling and commonly used event tree/fault tree techniques fail to address known influences on human performance and the interrelationships between the plant and its human operators.

A PRA model is constructed to identify and estimate the frequencies of the scenarios that lead to core damage, or other undesirable plant states. The systems analysis approach to constructing a PRA model is essentially one of decomposition that results in a scenario being defined in terms of an initiating event combined with a minimal set of equipment unavailability states. In this sense, the appropriate level at which to include human failures, are either contributors to initiating events or to equipment unavailability states. Thus, specific human failure expressions resulting from erroneous actions either in the pre- or post-initiating event phases can be identified with modes of unavailability of functions or specific items of equipment. Stated simply, erroneous human actions have the effect of initiating an accident sequence or rendering equipment unavailable that may protect against or mitigate the consequences of the initiating event. As was observed in the data survey discussed in the draft BNL and SNL reports, one erroneous action often is associated with several such effects.

The PRA can be performed for the whole spectrum of plant operating states. Each operating state defines the functions that have to be maintained to remain in that state. An unplanned disturbance that causes a degradation of those functions, which in turn demands some mitigating function to be performed, can be identified as an initiating event. The mitigating functions define the set of essential equipment necessary to protect the plant against radioactive release. Thus, from a knowledge of the plant status and the plant's particular configuration within that operating status (which may be especially important in LP&S phases), the set of equipment which must be maintained in an operable condition can be defined. The possible failure modes, or modes of unavailability, of this set of equipment provides the domain over which potential human failure expressions should be defined. The identification of these unavailability modes is the purpose of the concurrent projects at BNL and SNL to estimate the levels of risk associated with LP&S activities. The nature of PRA, and the constraints and requirements PRA imposes on HRA methodologies, is discussed further in Appendix A.

Ultimately, the systems analyst needs: (1) guidance on how to search this potential set of failure modes to identify the most risk significant human failure expressions for inclusion in the model, (2) guidance on how to incorporate these human failure expressions into the model, and 3) guidance on how to estimate the appropriate failure probabilities. The development of such guidance is the central purpose of the methodology development part of this program.

2.2 An Improved Human Performance Modeling Process

Section 2.2.1 outlines what will comprise the improved human performance modeling process in terms of the areas for which it will provide guidance and on what that guidance will be based. Section 2.2.2. outlines the development work required to create this improved process.

2.2.1 Contents of an Improved Human Performance Modeling Process

Any complete method for modeling human performance must consist of three basic steps. First, it must provide guidance to the analysts as to what kinds of failure events influenced by human performance are to be considered as potentially important to risk. For example, standby equipment being unavailable when demanded is a major category of failure events, which can be caused by human errors such as failing to restore equipment following testing. This guidance is used in selecting events to be included in the systems models (the fault trees and event trees) that define the combinations of failures leading to unacceptable outcomes like core damage. This step is commonly identified as screening.

Second, it must provide guidance to the analysts on how to combine human performance and equipment reliability in such a way that the resulting risk calculations are reasonable representations of the combined performance. For example, which human errors cause system failures directly, which require combinations of human errors and equipment failures, and how human actions can recover failed equipment to prevent systems failures. In addition, human errors and system behaviors can interact to cause unusual hazard states, which then require analysis. This is called the representation step.

Finally, the method must provide guidance on how probabilities associated with the failure events developed in the representation step can be quantified. Often, either information associated with specified performance shaping factors (layout of indicators and switches, number of steps in a procedure) or historical data (numbers of failures in simulator trials, numbers of times valves found in wrong position) are used as the basis for this step, called quantification.

Figure 2 indicates this combination of steps and their inputs as they are currently used. However, as discussed in Section 2.1, these methods yield results that have significant limitations, especially in the context of low-power and shutdown operations. In order to remove these limitations, this program is intended to develop a new approach that extends the capabilities of these previous methods to take better account of historical data, and to be based more soundly on the emerging theories on the causes of human error mechanisms.

This new approach will still employ the same steps (screening, representation, and quantification) but will take into account more information. This should result in more realistic risk estimates and settings other than that of full power. The new approach is outlined in Figure 3.

In this approach, the guidance in screening step will take account of human performance strengths and weaknesses in performing tasks, and our emerging understanding of the causes of human errors. This additional information will provide a basis for extending the scope of modeling to include, for example, initiating events caused by human-system interactions.

The guidance provided in the representation step will take account of the additional inputs from the causes of human errors to guide, for example, which human errors should be considered as "common--cause" events transcending failures of individual components or systems. This guidance will identify where, in the systems models, different kinds of errors should be represented.

The final area to be improved is the quantification step. In the past, existing methods have taken one of three approaches. These were: (1) the use of look-up tables that relate probabilities of failure to task characteristics ("performance shaping factors"), (2) the use of algorithms to compute probabilities of failure based on some kind of timescale, or (3) the use of subjective estimates, either directly or using intermediate factors. These approaches will be augmented by using plant (not simulator) experience more focused on the specific activities of concern. This will be accomplished using knowledge of the causes of human error to identify which are the most important factors that influence error rates. The guidance for quantification will be in the form of a procedure that will require elicitation of expert
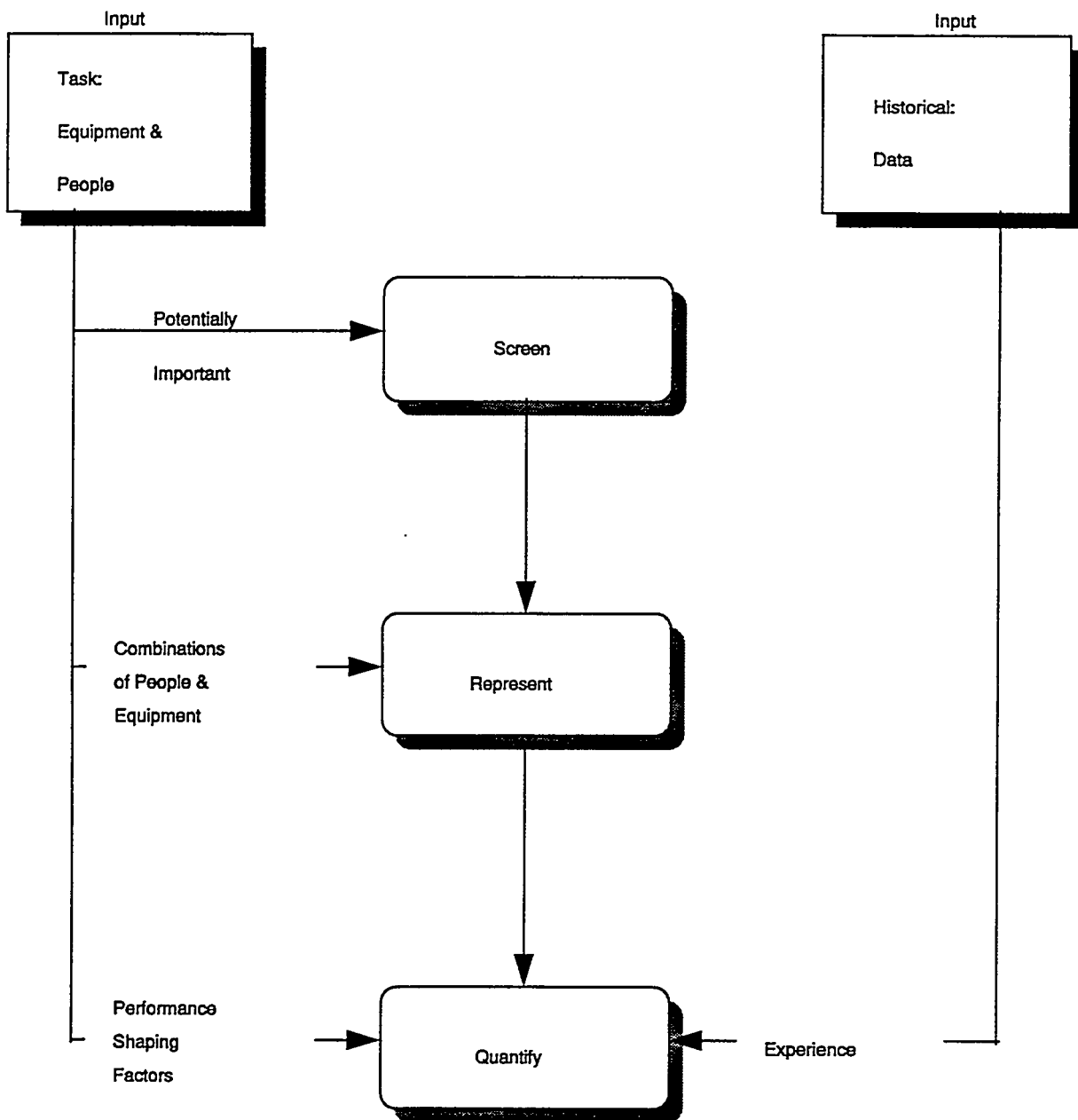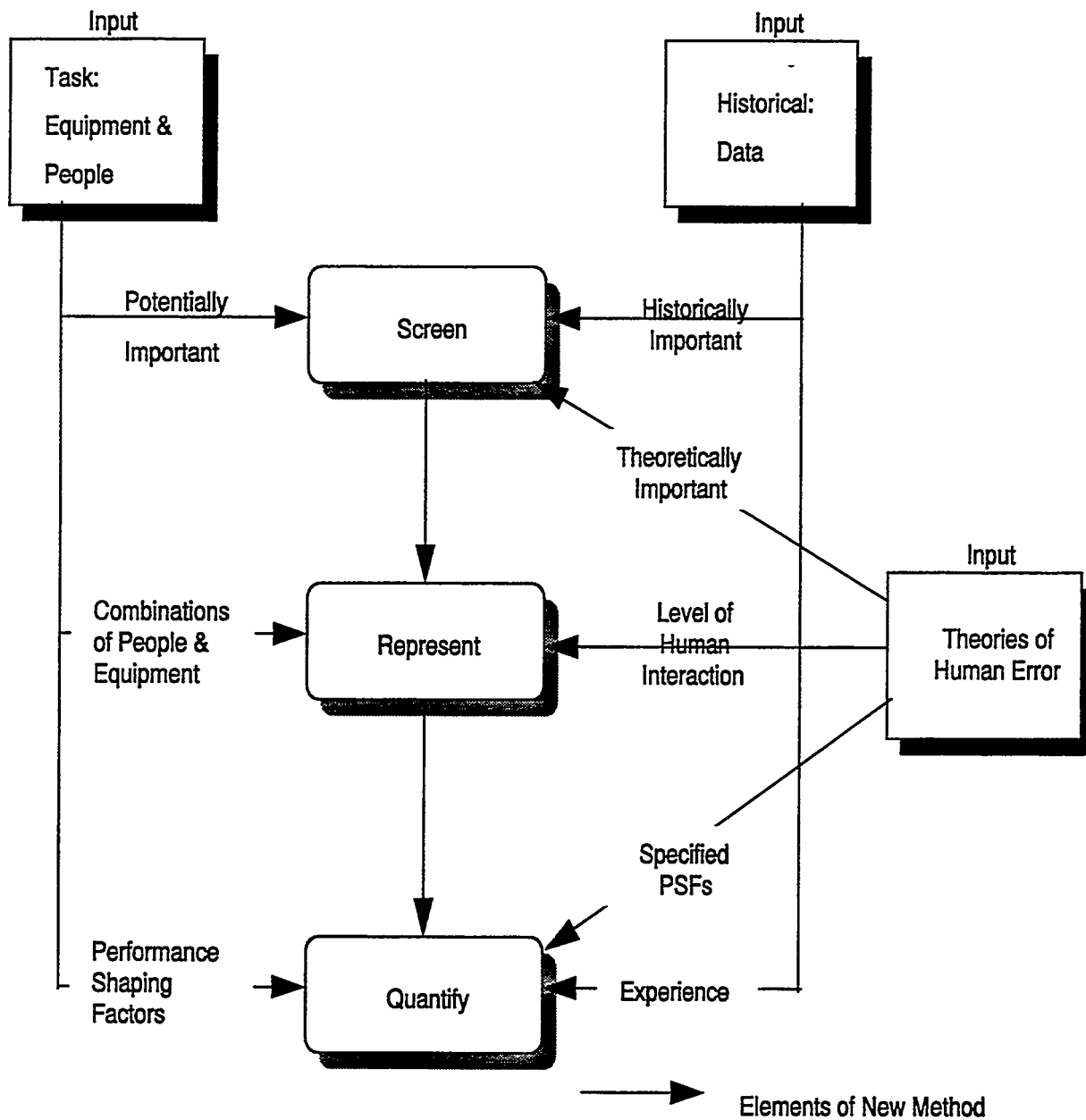
Figure 2. Form of Existing Analysis Methods

Figure 3. Form of new analysis approach

opinion; this elicitation will evaluate the factors identified as important in the underlying theories of the causes of human error. Such an approach will also take into account the observation that, in many cases, the factors influencing the error rates are not simply linear and separable, but can be complex and interactive.

2.2.2 Development Process of an Improved Human Performance Modeling Process

In order to create the improved modeling process described above, development in several areas is required. The first step in the development process is to identify the needs of the intended users, such as their specific needs, what tools they would expect to use, resource availabilities for applications and so on.

Three methodological development tasks are planned. These tasks are: (1) development of a human error framework (that is, a description of how causes of human errors relate to their influence on systems reliability models), (2) development of means for screening and representing errors of commission and other (currently unrepresented) failure modes in systems models, and (3) development of appropriate quantification processes. These tasks are described in greater detail in Section 2.3.4. One further task is the development of methods for modeling scenarios found to be important in data but beyond the scope of present techniques. One such case is the interaction of equipment being operated during concurrent testing or operation of multiple systems. Such situations were found to be important during low-power and shutdown operations as initiating events, for example.

The products of the development process will be implementation guidelines for screening, representation, and quantification. These guidelines will be sufficiently detailed for the intended users to be able to use this improved modeling process to perform more realistic risk studies. A final task in the development program will be a series of trial

implementations by the intended users leading to a final published product.

2.2.3 Planned Approach

This work is planned to be performed in a total of six major tasks, of which five are planned to take place in this next phase of the project. The first five tasks represent the development activities; the sixth task is trial use by intended end-users. These tasks are shown in Figure 1. Task 1 is the preparation and presentation of the results to date from the data surveys by both BNL and SNL into a single integrated report, and the incorporation of this program plan as an intermediate report.

Task 2 is the identification of user requirements from the final program plan methodology; the task includes interviews with prototypical end-users about the kinds and levels of guidance required, constraints imposed in terms of technological aids, and so on. Task 3 is the development of an HRA framework to serve as the unifying skeleton for subsequent development tasks. It incorporates knowledge from the fields of psychology and human factors engineering in a way the can be related to the requirements of the PRA process.

Task 4, the largest effort, is composed of four research and development tasks. Two of these four tasks are concerned with developing guidance for incorporating human failure events appropriately into the PRA systems modeling activities; this includes representation of "errors of commission" and evaluation of other dependence mechanisms. Such guidance would include how to model human-caused initiating events, how to identify and incorporate multiple consequences of failure, and how to search for the most "error-likely" situations. The third task is to develop a systematic approach for quantification of human reliability. The final task is to develop integrated methods for evaluating scenarios that may arise from the unforeseen interactions of multiple plant activities, such as two simultaneous tasks involving vessel draindown that are uncoordinated.

Task 5 is the development of guidelines to apply the methods, developed in Task 4, by the intended users identified in Task 2. Task 6 is the trial application and refinement of these guidelines.

2.3 Description of Program Tasks

2.3.1 Task 1: Provide Interim Report

Prepare a draft NUREG/CR document that: (1) summarizes the information contained in both the BNL and SNL draft letter reports produced in Fiscal Year 1992, (2) presents the program plan for the RES IMPROVED PRA, (3) describes the connection between the information summarized in (1) and the program plan presented in (2), and (4) documents both the BNL and SNL draft letter reports in separate appendices. A draft outline of the NUREG/CR document will be submitted to the NRC Project Manager for approval.

2.3.2 Task 2: Identify User Requirements

It is critical to the success of the IMPROVED PRA that it be accepted by its users as a practical and easy to use tool that meets their needs for integrated assessment of human and equipment performance. In order to precisely define those needs and to better understand what the user considers practical and easy to use, this task will perform a focused assessment of user requirements. Those user requirements will help define specific design requirements for the model, and will be used later in testing and evaluation of the model to assure satisfaction of user needs. This task has three primary elements: (1) identify users, (2) collect information on user needs, (3) assess findings and develop specific model requirements, as follows:

1. The primary user has been identified as NRC staff and/or contractors who perform PRA. Other potential categories of users whose needs are to be assessed will be identified in concert with the NRC Program Manager. Other users might include other NRC staff involved in assessment of human performance, HRA/PRA practitioners in the nuclear utilities, or others in the nuclear

industry. Representative individuals will be identified for each category of user.

2. The collection of information will be accomplished by a structured interview. The project team includes representatives of the primary user group, namely lead HRA/PRA practitioners from Brookhaven and Sandia National Laboratories. This "in-house" expertise will be used to help develop an interview instrument and to produce an initial set of user requirements. Other representative users external to the team will be interviewed to refine and complete the information obtained from the team members. This approach will help to minimize the impact on interviewees and the team resources required to complete the interviews.

3. The input from all interviewees will be evaluated, and a final set of user needs will be documented for incorporation as "design requirements" for the IMPROVED PRA. The user-specified needs will be translated into specific, demonstrable requirements for the model. Those requirements will drive the development of the model, and will be the focus of testing and evaluation performed in the demonstration planned under Task 6. The user requirements are expected to address the types of support needed, acceptable and easily used formats for the information, constraints on user resources required, and other issues of practicality, acceptability and ease of use.

2.3.3 Task 3: Refine HRA Framework

The purpose of the HRA framework is to provide a logical and explicit basis for the development of rules for incorporating human-failure events into PRAs that are consistent with the knowledge about the consequences and rates of occurrence of different types of human errors. The framework should describe the relationships between human errors as considered in the behavioral sciences and the human failure events as considered in the PRA
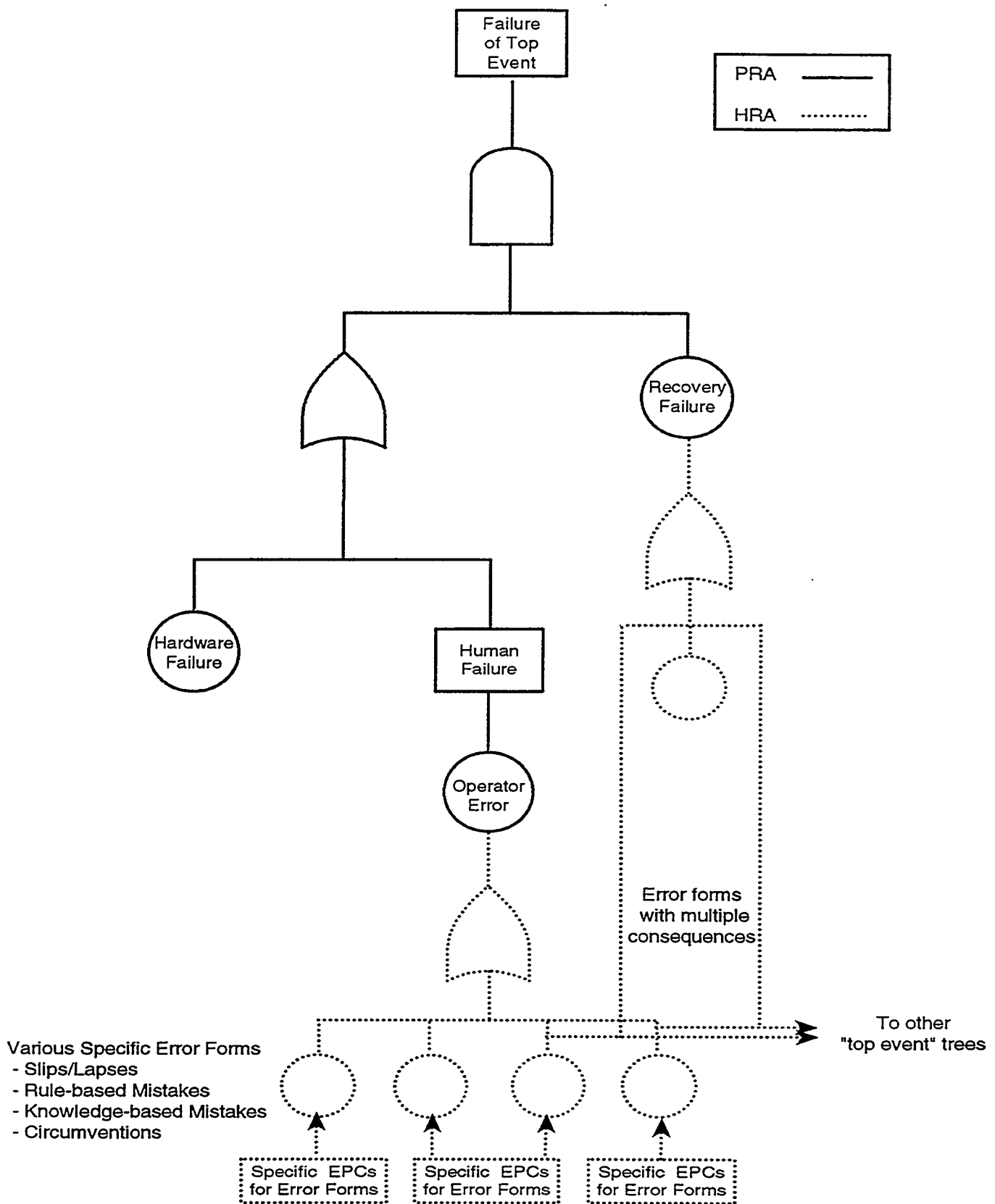
Figure 4. Concept of HRA construct

systems-analysis tasks. Figure 4 illustrates the concept of the proposed framework, showing how different kinds of errors become combined logically in different ways with hardware failures to yield system failures. Figure 4 presents a framework of human error based on information developed in the behavioral sciences. The selection of this framework is described in Appendix B.

Once described, these relationships will provide a basis for the development of guidelines on how to incorporate different kinds of human errors into the evaluation of the various human failure events. They should further provide an indication of the kinds of data relationships that will be required to produce a working HRA/PRA methodology. This task will therefore produce inputs to several of the components of Task 4, the research and development efforts. Tasks 4.1 and 4.2 (and to a lesser extent, Task 4.4) will develop guidelines for the representation of different types of human errors and their relationships to systems failure events into the PRA. Task 4.3 will develop guidelines for the quantification of human-failure events based, in part, on the important performance-shaping factors (PSFs) associated with the different types of human error identified in the framework. Table 1 summarizes the different types of errors and some of their key characteristics.

Existing HRA methods rarely state any specific relationships considered between different types of human error and how they affect systems failures. One of the most frequently used HRA methods, THERP, and its simplified derivative, the ASEP HRA method, are concerned primarily with one type of human error - slips and lapses. This error type is considered to be perhaps the least important in terms of risk, and were not found to be important in the previous data analysis. Other HRA methods similarly focus usually on only one type of error, and provide no guidance on the relationships of other error types to safety.

The development work required in this task is to use an existing framework from the behavioral sciences and extract from that an identification of the most important error types and their associated PSFs. The

selection of this framework to be refined is described in Appendix B. The identification of the most important error types will be based on the results of the earlier data survey and discussions with experts. Once identified, these error types will be evaluated in terms of how they may affect human performance in terms of systematic causes of failures important in the PRAs. For example, which error types are potentially important as mechanisms for the so-called "errors of commission" where multiple unsafe acts can result from a single error of intention. For those error types found to be important, principal PSFs will be identified from the literature for consideration in Task 4.3.

An important concern in this program is to limit the focus of potential error types and PSFs considered to those that have the potential for significantly influencing the levels of risk assessed in the PRA, i.e., "errors of commission" and other error mechanisms that may have multiple dependent consequences. Therefore, the findings of the earlier data survey (including the interviews) will be used to limit specific plant activities and error types examined.

2.3.4 Task 4: Research & Development Efforts

2.3.4.1 Task 4.1, Identify and Represent Errors of Commission

On the basis of the LP&S event and literature reviews conducted during Fiscal Year 1992, a significant number of LP&S events were identified which resulted from inappropriate human actions and led to undesired consequences with respect to plant functions. Given that such Errors of Commissions (EOCs) play a significant role in the LP&S environment and have the potential to decrease plant safety margin or precipitate an initiating event, it is essential for any HRA/PRA methodology applied to risk assessment during LP&S to include an approach for identifying, representing, and quantifying potential EOCs. Unfortunately, traditional HRA methods have provided only cursory treatment of EOCs and little

Tasks and Products

Table 1. Examples of Significant Error Types

Error Type	Characteristics	Example PSFs
Slips	Lack of attention, outcome not as intended (e.g., wrong switch selected and operated)	Workload Layout of panels, annunciators, etc.
Lapses	Memory failure, outcome not as intended (e.g., omitting step in procedure)	Workload Procedure design Training
Mistakes	Error in intention, usually carried out purposefully (e.g., misunderstanding problem, inappropriate solution)	Training Instrumentation Procedure errors
Circumventions	Inappropriate action taken deliberately, with no malicious intention (e.g, shortcutting procedure to simplify actions, such as reversing steps to avoid repeated movements)	Training Task design Supervision

or no guidance regarding the identification of EOCs for analysis in the PRA context.

Since the possibilities for inappropriate actions in a nuclear power plant are essentially unbounded, a method which constrains the search process for EOCs to a manageable level will be a critical aspect of an IMPROVED PRA methodology. PRA analysts and modelers will need a guide and a set of screening rules which provides them a relatively straightforward means of identifying particularly error prone situations and scenarios and a means of quantifying the potential occurrence of the human failure events.

While several recent efforts have made attempts to address EOCs at some level, e.g., SNEAK, INTENT, it is argued that these methods provide only general guidance for identifying and quantifying EOCs. For example, while the SNEAK approach may in fact facilitate the process of isolating potential EOCs, the approach still requires a more or less unbounded analysis of plant systems and potential operator interactions in order to identify EOCs. No guidance is given regarding "where" to apply SNEAK or how to constrain the search process. Similarly, while

INTENT may be useful in categorizing previously identified errors of intention in ways that allow estimates of error probabilities to be derived for some situations, no help is provided in identifying where or under what conditions EOCs are likely to occur.

Two different, but related tasks will be required to develop the methodology for identifying and representing EOCs. One task focuses on identifying the causes of human errors in order to understand how these errors will be expressed in terms of their impact on plant functions. The other takes more of a systems analytic approach and attempts to develop guidelines for identifying where opportunities exist for inappropriate human actions which could lead to interference with plant functions. The results of these tasks will also provide input into the development of an applicable quantification methodology (Task 4.3) and into the identification and representation of dependencies (Task 4.2).

The first task will be based on the development of the framework discussed in Task 3 above. The goal will be to use the framework as a basis for developing a predictive model of human error,

D-13   NUREG/CR-6093

which will in turn be used to develop a set of rules which PRA/HRA analysts can use to recognize conditions likely to produce inappropriate human actions. Through the use of a model based on current understanding of the "laws of human behavior," it should be possible to determine the types of errors which are likely to occur in specific situations, the likely causes of those errors, their potential consequences, and their related dependencies.

The second task assumes that one basis for the identification of EOCs for use in risk assessments would be a thorough examination of the circumstances under which EOCs have occurred previously and the nature of their consequences. The "product" of such an examination would be a set of guidelines for identifying opportunities for inappropriate actions which could have important consequences in regards to plant functions. Thus, the HRA/PRA analysts would have a guide that allows a screening for the events of greatest concern. An obvious benefit of such a guide is that at least the first iteration of a search for EOCs could be constrained on the basis of the kinds of EOCs that have occurred in similar environments.

Since there is little existing data available on post-accident human errors, a somewhat different approach will be needed for obtaining data relevant to identifying EOCs which might occur during accident scenarios. One possibility would be to conduct interviews with operators, operations training personnel and other experts regarding confusion factors and potential misinterpretations that might be confronted by operators in various accident scenarios. The results of such interviews would at least capture current concerns and provide starting points for identifying potentially critical EOCs.

Clearly, there are many levels to which the above approaches could be taken. Given the current time frame for development, the program will have to constrain itself to developing methods which will capture and represent the more critical inappropriate human actions possible in PRA space.

2.3.4.2 Task 4.2, Develop Approach to Deal with Dependency

In the modeling of the human/system interactions, events are introduced into the logic model to represent failures or other modes of unavailability of equipment as a direct result of human interactions. A scenario description or an accident sequence cut-set may contain several such events. This issue is concerned with developing approaches to ensure that any dependency between these logic model events is identified, and to correctly capture the probabilistic impact of this dependency.

The dependency between events arises largely because errors, or other human failures, are modeled in terms of their consequence for items of equipment rather than on the basis of cause. This makes sense from the point of view of developing plant logic models in terms of equipment states. However, if the human failures that result in unavailabilities of several pieces of equipment, have a common cause, the logic model events representing the impact of those errors are not independent.

If the dependence between these events is not treated correctly, the risk profile obtained from the PRA will not be accurate. Those scenarios involving multiple human error related events can be inadvertently truncated from the model if the events are treated as independent, when in reality they are dependent.

The issue may be more significant in low power and shutdown phases because of the greater potential for affecting multiple phases of the accident. For example, a human error that causes the loss of an initial function, such as maintaining inventory, may be the result of a mechanism that increases the likelihood that recovery of that function will not be successful. In the full power modes, by contrast, apart from initiating events caused by loss of support systems, the equipment required for response to an accident is largely independent of that whose failure causes the reactor trip, and this across-phase dependency may not be so important.

Current PRA approaches to human error treat the human error events as failure modes, e.g., operator fails to initiate system. The causes of the error are rarely explicitly modeled, even qualitatively. The issue of dependency is treated at a fairly superficial level, often using a formula for evaluating conditional probabilities based on a subjective assessment of the degree of dependence between the events. There is little explicit guidance on how to identify when events should be regarded as being dependent, nor on how to establish the degree of the dependence. The formula used for conditional probabilities has no theoretical basis.

The approach to this problem is to use the framework to investigate possible "causes" of errors as a function of the activities performed by operations and maintenance personnel. The causes, expressed as "performance influencing factor" (PIFs) or error producing conditions (EPCs) will be a function of the mode of human error. Based on this breakdown, consideration will be given to approaches for representing and accounting for this dependency, which may take one of two forms. The first is an explicit breakdown of events into "causes," the second is a quantitative approach similar to that used in common cause failure analysis.

2.3.4.3 Task 4.3, Develop Quantification Process

The quantification process is the primary machinery of the IMPROVED PRA. If theoretical frameworks and principles of behavioral science are the framework, then the quantification process is the engine/drive-train. It provides a means to identify causal factors of importance, model the interre-lationships of those factors, estimate the impacts of those combined factors on human error, and produce a quantitative estimate of human error at the level required within the integrated human-systems analysis.

During Fiscal Year 1992, there was identified potentially important to HRA models for all states of operation, but especially for LP&S operations, that are not well addressed by current quantification processes. Among the most significant of those

issues are three that are addressed as separate tasks in this work plan:

- Treatment of errors of commission
- Treatment of dependencies among human actions/errors
- Treatment of multiple concurrent tasks.

In addition to these three there are other technical issues inherent to the HRA modeling process, such as interrelationships of influence factors, that are important to resolve in order to improve the existing methodology. Finally, there are important user-related issues, such as the need for more practical guidance and simple, operational definitions of influence factors, that need to be addressed to help assure that human reliability considerations are effectively incorporated into the PRA. For these reasons, a different quantification process is being developed in this task. The paragraphs that follow discuss the requirements for this new process, in the context of needed improvements over existing methods, and the approach planned to develop the new process.

There are a number of existing structures, techniques, models and approaches for quantification of human reliability. And there have been a number of critical reviews over the past several years by individual authors and industry or government sponsored groups of experts. The strengths and limitations are fairly well documented. A recent example is the report by the Advisory Committee on the Safety of Nuclear Installations of the British Health and Safety Commission, which reviews most of the best known methods, including THERP, HCR correlation, time reliability correlations, SLIM, HEART, influence diagrams approach, absolute probability judgment, paired comparisons, TESEO, MAPPS, and the WASH-1400 data base. While there are some specific relative strengths and limitations of the various methods, there is a underlying problem of lack of data, and hence lack of "predictive validity" faced by all methods that is the central criticism of most reviewers. Indeed, the field of human reliability has been noted by its founders and proponents, as well as by its detractors, for an extraordinary inability or unwillingness to

address the issue of validation of models by "hard data." If this is true, why is it true? The answer seems to involve both basic theoretical issues about the approaches to quantifying human behavior as well as practical issues.

The practical issues are obvious, and most frequently cited. They include the enormous number of factors possibly affecting human performance, the difficulty of obtaining "in-situ" measurements on people while the system is in operation, the lack of "realism" of laboratory experiments or simulator exercises, difficulties with obtaining direct measurements of human behavior (e.g., of cognitive tasks), etc. These practical factors, and others such as the difficulty of assuring sustained funding over the long period of years necessary to accumulate a significant statistical base, make it extremely difficult to maintain viability of such data collection projects.

These practical issues are not independent of, in fact are essentially just representations of, a number of fundamental theoretical issues, all of them basically having to do with whether it is appropriate to treat human reliability in a manner similar to machine error, as is done in the PRA framework. Adams describes four specific ways that human and machine error differ: (1) human errors cannot be assumed to be independent, yet the unique factors that affect each instance of human behavior are difficult to capture and quantify, (2) humans monitor their own behavior in a given situation and are able to correct error before the error affects system performance; thus, the probability of human error may be quite different from the probability that the human error induces a system error, (3) human operators do not function independently of each other; behavior is influenced by the behaviors and decisions of other operators; and (4) it is difficult to integrate human and machine reliabilities to come up with a joint reliability measure of the total system, because the reliability of the system will alter the probability of human failures in uncertain ways.

A critical point is that human behavior is highly context-specific. Each instance of human behavior is unique. Typical HRA approaches assume that this can be accounted for by numerically adjusting some

"basic" human error probabilities to account for these context-specific variations. Context-specific human behavior at a higher level (such as a control room crew diagnosing and responding to an accident event) is decomposed or disaggregated to a set of more basic human actions. Error probabilities are obtained from data sources that are intended to be more nearly context free. Then these basic error probabilities are multiplied by numerical values estimated for the influencing, or "performance shaping," factors and combined according to rules of logical operators, to arrive at the estimate for the higher level behavior. There are several basic problems with this approach, from the perspective of behavioral science critics.

First, there is a basic theoretical concern that human behavior, especially in higher level tasks, cannot be properly modeled atomistically in this fashion; that the "whole" is different from the (probabilistic) sum of the parts. Second, there is the more practical issue that all of the numerous performance shaping factors act together in a dynamic, inter-dependent, and usually non-linear fashion to influence the overall performance, and this interaction is far too complex to be well represented by simple, independent, linear factors. Further the relative "importance" of the various factors and the ways that they interact with other factors varies with the basic nature of the human action/error involved and, again, the context in which the human action takes place. Third, many of the influencing factors identified by behavioral scientists as important in shaping human behavior do not act in a direct and traceable way to influence a specific human action as it is desired to be modeled in the PRA framework. Factors such as individual level of knowledge, organizational factors, supervisor expectations and many others that are identified as potentially important influence behavior in more diffuse ways, sometimes cumulatively over time and in indirect ways that are too complex to "map" to a particular human action. Finally, there are issues cited by Adams having to do with "dependency" of human behavior - dependency of tasks in a sequence as discussed under Task 4.1, dependency on task and situational variables, dependency on other

humans and organizational influences, dependency on system response, etc.

Some other approaches, usually limited in scope, do not attempt to model explicitly the impacts of the various influencing factors in any detail; they simply present data taken *in context* and leave it to the user, perhaps with some general guidance, to extrapolate from the data context to the user's own particular application of interest. Several "models" based on simulator data in the nuclear industry are examples (e.g., HCR, and time reliability correlations). Still other approaches, such as HEART are essentially compilations of quantitative values of error probabilities based on judgment and experience in particular contexts with some general guidance for extrapolation or generalization to the user's task/context. SLIM and similar methods attempt to account for specific influences in context, but have to rely on fairly intensive interaction of behavioral specialists and operations/systems experts for each investigation, preferably in the context of interest, to arrive at "high quality" information. These approaches also require significant control and resources to reduce variability of estimates. Thus, while the existing approaches to quantifying human reliability have varying strengths and limitations, all have been inhibited by this underlying problem of lack of data. And, consequently, all are essentially subjective approaches. They offer a means for codifying expert judgment, for guiding users to make expert judgments, or for reducing variability among expert judges. The state of the art does not yet provide a rigorous theoretical or empirical structure.

There is nothing inherently "wrong" with obtaining data and information from experts. Indeed there is far more subjectivity in most engineering and technical systems analysis than many technical personnel recognize, or admit. From a user's point of view, however, practicality of many of the approaches is limited because they require highly experienced specialists. Scrutability and reproducibility by other analysts also are limited. Justification of numerical values estimated by the expert is difficult. In brief, the field is viewed as more of an art practiced by a small handful of

consultants than a science or engineering discipline with a substantive theoretical or empirical basis accessible by intelligent users. This presents difficulties for users and a lack of "respect" for the work in the field.

From this assessment of the state of the art, several critical requirements or desired characteristics for the proposed quantification approach become apparent:

1. The IMPROVED PRA approach must recognize that the method will have to be fundamentally subjective. Every available source of data - historical records (e.g., LERs, root cause analysis, incident reports, investigations, inspection reports), data stores such as NUCLARR, simulator data, etc., *and expert opinion* should be pursued to "validate" the judgment of experts; but the state of the art and the practical difficulties discussed above dictate that the quantification approach will be based largely on expert judgment.

2. The human behavior of interest must be examined in context. Identification of the important influence factors, the relationships among the influence factors, and the relationship between influence factors and error expressions must be examined in the context of the nuclear plant systems, tasks, and environment.

3. A corollary to Item 2 above is that the experts from whom information is elicited to identify and quantify the model relationships must include nuclear plant operators and systems analysts. These experts can make operational definitions of the key factors that influence performance on the job. The results of the elicitation and model development process need to be consistent with the theoretical base of knowledge in behavioral science (i.e., with the *frameworks* discussed earlier in this plan). However, the experience from application of existing models is that in order for the model to be a practical success, the factors must be expressed in operational, "observable" terms.

4. The quantification approach needs to be able to account for interdependence and non-linearities in the relationships between influence factors and error expressions.

5. The quantification approach, including the guidance provided with it, must have the expertise of behavioral science embedded in it in a way that is usable by the primary user, namely knowledgeable NRC PRA specialists. Highly specialized expertise in behavioral science, or resources beyond those likely to be readily available to the primary user, should not be required in order to interpret and effectively use the model. More specific user requirements for the model will be identified from the efforts described in Task 2 of this program plan.

6. The quantification approach should be able to accommodate and effectively represent the results of the R&D Tasks 4.1, 4.3 and 4.4 on errors of commission, dependencies, and multiple concurrent tasks.

7. The quantification approach should be structured to accommodate continuous updates and improvements based on results of data collection efforts. Also, it should be as flexible as possible to accommodate potential future modeling improvements in the field.

8. The development of the quantification approach, and the subsequent implementation of the approach should be compatible with, and should be supported by, a continuous effort to collect and analyze operational data and to "validate" the predictive capabilities of the approach.

An outline of an approach to produce the quantification methodology is provided in Appendix C.

2.3.4.4 Task 4.4, Develop Approach for Incorporating Multiple, Concurrent Tasks

During shutdown, many different activities are occurring in the plant at any given time. Although the control room (CR) typically has official control over safety-critical activities, it is still difficult to keep track of the status of activities since the plant configuration changes relatively frequently. The variety of tasks includes: (1) different personnel (e.g., auxiliary operators, I&C technicians, maintenance, system engineers, contractors), (2) different locations (e.g., the CR, local control panels, direct manipulation of components), and (3) different activities (e.g., testing, maintenance, configuration changes, housekeeping). As a result of the various activities going on during shutdown, there is the potential for unanticipated interrelationships between tasks via interfacing systems, support systems, and multiple locations for system manipulation.

Unanticipated interactions between seemingly unconnected tasks can result in an initiating event or in complications in responding to an accident. In both cases, a human error does not have to occur in order for an undesired sequence of events to occur. For example, two RHR vent valve test procedures, which if performed individually have no impact on safety, resulted in a loss of RCS inventory and loss of RHR when they were performed together (Braidwood 1, 10/4/90 event). On the other hand, activities in the plant may leave system, components, or instruments unavailable to use in response to an unrelated initiator. Such interactions have the overall effect of additional system, component, or instrument unavailabilities.

The issue of interactions between human activities in the plant, errors or otherwise, is not commonly addressed in PRAs. The dynamic nature of the plant during shutdown requires that this issue be addressed.

First, a process for identifying potential interactions between plant activities will be developed. Since, in some cases, interactions between multiple,

concurrent tasks occur because of inadequacies in planning, the identification of such interactions could be based upon reviews of outage plans and controls. Second, a method for representing the effect of these interactions must be determined. This task will develop several alternative representation schemes and recommend one for application that best meets the users' needs. Since interactions can result in either initiating events or equipment unavailability, representation in the PRA model is expected to impact both event trees and fault trees. Third, the probabilities of adverse effects from these interactions must be quantified. This task will be supported by other tasks in the program (e.g., review of historical data, development of HRA quantification methods, etc.).

2.3.5 Task 5: Develop Implementation Guidelines

The objective of this task is to develop detailed implementation guidelines for the performance of the IMPROVED PRA. These guidelines will provide a hierarchical description of the HRA/PRA 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 by the intended users and (2) produce well documented, auditable results. To meet these requirements, the guidelines must be concise and explicit and must provide the necessary tools and data to perform all phases of the analysis.

The organization and format of the guidelines will be determined based on the user requirements defined in Task 2 and the results of the development efforts performed in Tasks 3 and 4. It is anticipated that the guidelines will be organized in a hierarchical structure corresponding to the major stages of the IMPROVED PRA process. For each phase, the overall objectives, technical bases, and outputs would be described. Within each phase, detailed guidelines will address the specific activities to be performed. These detailed guidelines would describe the methods, tools, criteria, and data for performing the activity. Suggested formats for documenting the results would also be provided.

A four-step approach will be used for development of the IMPROVED PRA implementation guidelines. The first step is a specification of requirements for the format and style of the guidelines based on the results of Task 2, Identify User Requirements. An overall process description and flowchart for the guidelines will be developed based on the results of the framework development in Task 3. This flowchart will define the stages of the process and identify the activities for which detailed guidelines will be prepared.

The second step is the development of detailed guidelines. The detailed guidelines will be prepared based on the results of the developmental efforts in Task 4. For activities where additional development work is not required, the guidelines will be based on existing methods and data as documented in the literature. These detailed guidelines will be integrated into a draft guidelines document. The guidelines will be applied to example problems taken from the LP&S PRA studies as well as previous IPEs. The results of these sample analyses will be used to refine and modify the guidelines and may be incorporated as case studies in the final document.

The fourth step in the development of the guidelines will be a peer review. This review should include experienced PRA analysts from the intended use population. A structured review process will be used to gather the comments and recommendations of the peer review. These results will be incorporated into the draft guidelines document prior to the full scale demonstration in Task 6.

2.3.6 Task 6: Demonstrate Guidelines

The objective of this task is to evaluate the draft guidelines developed in Task 5 by testing and revising them in a trial application by PRA/HRA analysts. The evaluation will be used to demonstrate the usefulness and understandability of the guidelines including their ease of use and consistency with expectations and other PRA/HRA results.

Tasks and Products

The demonstration will be performed by a trial application of the draft guidelines on an appropriately selected initiating event for a PWR and a BWR from each of the Level 1, Phase 2 LP&S Projects (FIN Nos. L1922 and L1923.)

Based on the feedback of these test results, "lessons learned" are anticipated being made. As a result, the guidelines will be refined to enhance their usefulness and effectiveness. Also, the feedback will help determine the possible need to examine one or more other LP&S initiating events.

3. Program Management, Guidance, and Reporting

3.1 Program Management

Overall program management at the NRC resides with the Office of Nuclear Regulatory Research (RES) Project Manager (PM), A. Ramey-Smith. Both Brookhaven National Laboratory (BNL) and Sandia National Laboratories (SNL) will be responsible jointly to the NRC PM via their respective Principal Investigators (W.J. Luckas, Jr. for BNL's FIN L2415 and D.W. Whitehead for SNL's FIN L2539) for the management of their respective assigned portions of the program plan including its development, testing and implementation.

3.2 Peer Review Guidance

It is anticipated that there will be established an external peer review group to periodically review, comment on and monitor the progress of the development, testing and implementation of the program plan. This group will act as an independent oversight body to this program similar to that performed by the LP&S Senior Consulting Group.

3.3 Reporting Requirements

Several types of reports will be used to monitor and document the progress of this program. These include monthly business letters and technical reports in the form of task letter reports and NUREG/CR reports as appropriate with the completion of key tasks as specified below:

3.3.1 Task Letter Reports

(1) User Requirements and HRA Framework Report

At the end of Tasks 2 and 3 (estimated to be less than 3 calendar months after program start), a draft letter report will describe the identified user requirements and refined HRA framework.

(2) Individual Research Issue Reports

At the end of Tasks 4.1, 4.2, and 4.4 (each estimated to be less than 12 calendar months after start), a draft letter report for each research and development task will describe individual research issue and associated findings.

3.3.2 NUREG/CR Reports

(1) Human Reliability Model Needs and Program Plan (Interim) Report

At the end of Task 1 (estimated to be 3 calendar months after program start) with input from concurrently performed Tasks 2 and 3, a draft NUREG/CR will describe the program plan being implemented and summarize the human reliability information related to low power and shutdown activities contained in both BWR and PWR FY92 draft letter reports.

(2) Research Issues and Draft Implementation Guidelines Report

At the end of Tasks 4.3 and 5 (estimated to be 12 calendar months after program start) with input from Tasks 2, 4.1, 4.2, and 4.4, a draft NUREG/CR will detail the concurrently performed research and development efforts of Task 4 and the resultant draft implementation guidelines of Task 5.

(3) Final Implementation Guidance Report

At the end of Task 6 (estimated to be 24 calendar months after program start) with input from Task 5 and "lessons learned" from trial applications, a draft NUREG/CR will detail the implementation guidance including final guidelines and examples based on trial application(s).

4. Program Schedule

4.1 Timeline and Milestones

The flow diagram developed and presented as Figure 1 identifies the relative time relationships among the various IMPROVED PRA program plan tasks. This figure also defines each task in the context of calendar time.

4.2 Deliverables

See Section 3.3 above.

4.3 Level of Effort

The estimated level of effort anticipated to be necessary to perform each of the tasks (described in Section 2.3) is provided below. Note that Tasks 1 through 5 are all planned to be completed within the first 12 months after the start of the project.

Task 1:	6 staff-months in 3 months
Task 2:	3 staff-months in 1 months
Task 3:	3 staff-months in 1 months
Task 4.1:	8 staff-months in 6 months
Task 4.2:	8 staff-months in 6 months
Task 4.3:	26 staff-months in 9 months
Task 4.4:	4 staff-months in 6 months
Task 5:	26 staff-months in 6 months
TOTAL:	**84 staff-months in first 12 months**

and for Task 6, TBD staff-months in second 12 months.

5. References and Other Footnotes

[1] NUREG-1449, "Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States," Draft Report for Comment, U.S. Nuclear Regulatory Commission, February 1992.

[2] NSAC-52, "Residual Heat Removal Experience and Safety Analysis, PWRs," Electric Power Research Institute, January 1983.

[3] "An Assessment of Human Reliability Influences During Low Power and Shutdown Conditions in PWR Nuclear Power Plants," Revised Draft Letter Report, Brookhaven National Laboratory, October 9, 1992.

[4] "An Assessment of Influences on Human Reliability During Low Power and Shutdown Conditions in BWR Nuclear Power Plants," Draft Letter Report, Sandia National Laboratories, October 9, 1992.

[5] The causes of failure include, but are not restricted to, types of human error.

[6] Hahn, H.A., Blackman, H.S., and Gertman, D.I., "Applying SNEAK Analysis to the Prediction of Human Error," Reliability Engineering and System Safety, 33 (2), 289-300 (1991).

[7] Gertman, D.I., Blackman, H.S., Haney, L.N., Seidler, K.S., and Hahn, H.A., "INTENT: A Method for Estimating Human Error Probabilities for Decision Based Errors," Reliability Engineering and System Safety, 35, 127-136 (1992).

[8] Advisory Committee on the Safety of Nuclear Installations, Study Group on Human Factors, "Second Report: Human Reliability Assessment - A Critical Overview," Health and Safety Commission, London, 1991.

[9] Adams, J.A., "Issues in Human Reliability," Human Factors, 24, 1-1.

[10] Summarized in Parry, G.W. et al., "An Approach to the Analysis of Operating Crew Responses using Simulator Exercises for use in PSAs," in Proceedings of the OECD/BMU Workshop on Special Issues of Level I PSA, GRS-86, July 1991.

[11] The data may or may not be directly accessible through the sources used in HACS.

[12] See, for example, Rasmussen, J., "Information Processing & Human-Machine Information: An Approach to Cognitive Engineering," New York: North-Holland, 1986.

[13] Reason, J., "Human Error," New York: Cambridge University Press, 1990.

[14] Woods, D.D., Roth, E.M., and Pople Jr., H., "Cognitive Environment Simulation (CES): An Artificial Intelligence System for Human Performance Assessment," NUREG/CR-4862, Pittsburgh, PA: Westinghouse Electric Corporation, November 1987.

[15] See, for example, Boff, K.R., Kaufman, L., and Thomas, J.P., "Handbook of Perception and Human Performance," Vol. II, New York: Wiley Interscience, 1986, pp. 41-49.

[16] Reason, J., "The Cognitive Worm at the Core of the TRC Model, Panel Session, HRA: Where Goest Thou?," Annual Meeting of the Human Factors Society, Orlando, FL, July 1989.

[17] Connelly, E.M., "The Theory of Human Performance Assessment," Proceedings of the Human Factors Society, 198x.

Appendix A. Issues Associated with the Integration of HRA into PRA

A limitation of current PRA models is that they tend to model events as success/failure, i.e., binary on-off states, and in particular, though it is not impossible to do so, the dynamic development of scenarios is not often treated completely. The fault trees, for example, are to a large extent static representations; temporal aspects of accident development can, however, be build into event trees. An important feature of modeling human/systems interactions is their dynamic nature. Failures, in a PRA context, are failures of a process, and that process, in most cases, allows recovery from an initial error, partly because the inertia of the system does not lead immediately to failure of vital equipment, or to an irreversible plant state, and therefore the operators have the possibility of receiving feedback from the plant, which allows them the opportunity to recognize and recover from errors. To complete the modeling of human/system interactions, and to allow the estimation of the probabilities of failure expressions, it is therefore important to incorporate recovery mechanisms. Since different failure expressions may result in different system responses, the feed back to the operators will also be different, and this will impact the potential for recovery. The potential for recovery is also a function of the failure cause and particularly if it is an error, the error form or mechanism. For example, errors of intention are generally felt to be less likely to be recovered than are simple slips.

A further limitation of PRA models, and in particular the HRA input, is that they have great difficulty in dealing with the dependence between human failure events. Since there may be some underlying common "causes" of failure, individual human failure expressions cannot, a priori, be regarded as being independent.

There are two important activities performed in HRAs. The first is the identification of opportunities for human interaction, which provide the opportunities for failure. The development of guidelines for identification of opportunities for failure, is expected to be relatively straight-forward, and will be based on an understanding of the various activities taking place at the plant. The work described below will facilitate the screening of the most risk significant failure events, thus allowing the analyst to keep the logic model from becoming too large and unmanageable.

The second activity is the quantification of the human failure event probabilities. The considerations discussed above suggest that an HRA model should recognize that different human failure "causing" mechanisms may be affected by different Performance Influencing Factors (PIFs) and that they have different recovery potential. One model having some of these characteristics has been reported in EPRI TR100259.[10] In a model based on this consideration, a human failure expression is the logical sum of contributions from several failure modes, which in turn can result from several failure mechanisms modified by appropriate recovery mechanisms. The challenge then is to take what is available from current developments in the cognitive science literature and adapt it as a basis for the development of a predictive model of human failure in a PRA context. The result of this is what in this document is called the HRA construct, and the use of such a construct is described briefly below.

The work of J. Reason provides an example of a 'model' of the cognitive process. Using Reason's S/R/K-performance structure, GEMS, and the associated error modes and error forms, it should be possible, using this 'model' to construct failure mechanisms for specific types of failures (or human failure expressions) that are related to the activities during all phases of plant operation and which are relevant from the point of view of a PRA. This issue is discussed in Appendix B. Then, it is necessary to try to identify what factors influence these mechanisms and how. For example, take a failure event in PRA space, operator terminates operation of pump "x" at an inappropriate time. The development process would work somewhat in the following fashion.

---

[10]Summarized in Parry, G.W. et al., "An Approach to the Analysis of Operating Crew Responses using Simulator Exercises for use in PSAs," in Proceedings of the OECD/BMU Workshop on Special Issues of Level I PSA, GRS-86, July 1991.

1. What error forms or mechanisms reasonably could be expected to lead operators to perform that erroneous act? For example, which error forms underlying the error modes inattention or overattention could be seen as leading to performing that act? Which error forms underlying the misapplication of good rules or application of bad rules? The same question would be enquired of the knowledge-based error forms.

2. The theoretical understanding in 1 may be supplemented by comparison with HACS reviews.[11]

3. The various error-producing conditions (EPCs) associated with these significant error forms should be identified

4. If possible, the EPCs should be expressed (or reinterpreted) in terms of potentially observable and auditable factors that could be evaluated prospectively in future PRA contexts.

5. For quantification purposes, the observable EPCs must be related to failure rates.

This latter task is probably only achievable by a formalized expert judgement approach. Thus one major development effort will be the establishment of a highly structured approach to the elicitation of the subjective judgements of experienced operating staff on the influence of the EPCs and combinations of EPCs on the likelihood of success, or of being misled. To assure the validity of this quantification approach, the development effort must include efforts and data for anchoring these judgments to operating experience.

Given completion of this work, an HRA model capable of recognizing the signature of particularly error prone situations or scenarios, and of providing a means of assessing the relative likelihood of the different ways in which errors may be expressed in different scenarios, will have been developed.

---

[11]The data may or may not be directly accessible through the sources used in HACS.

Appendix B. Selection and Use of an HRA Construct

B.1 Purpose

The purpose of the construct is to provide a basis for relating knowledge in the human error community to the needs of the PRA community. Each community has different concerns but use superficially similar terms, which has hindered the development of HRA techniques in the past. For example, the PRA community has included "human errors" as basic events in systems models. However, these are not human errors in the sense of the human error community; they are failures to accomplish some required hardware function, which may or may not be a result of a human error. For example, barriers to access equipment may prevent people from performing some action. Failure to accomplish that action is not an error in any meaningful sense. Specifically, the PRA community is concerned with failure events, not human error events.

However, human errors may cause failures of concern to the PRA community. (Historical experience, reinforced by the results of the earlier data analysis, shows that human errors may be the dominant cause of many failures that are important to safety.) Earlier HRA techniques have blurred the distinction between the consequences of errors and their causes by adopting a single consequence-single cause relationship. For example, a failure to restore a component after testing has almost always been considered the result of a slip (omitting a procedural step), and has been modeled using one HRA method that assesses the potential for slips, THERP. The blurring results in the expression of the THERP-assessed human error, "humans make slip while using procedure," as the PRA event, "failure to restore x after testing." The error may cause the failure, but so may other causes, such as a

deficiency in the task procedure. Causes and consequences are connected but they are not identical. One important function of the construct is to provide a means of relating human errors (as causes) to failures in the PRA systems models (as consequences) on a sound basis. Figure B.1 indicates these transitions.

If this relationship can be established, then two important parts of the integrated PRA/HRA technology can follow. First, there is a rational way to identify the potential multiple consequences (like "errors" of commission - actually consequences of commission) of errors such as mistakes that involve errors in intent formation. Second, there is a rational basis for evaluating the performance-shaping factors (PSFs) for each human error cause. For example, the PSFs associated with slips or lapses are substantially different from those associated with mistakes.
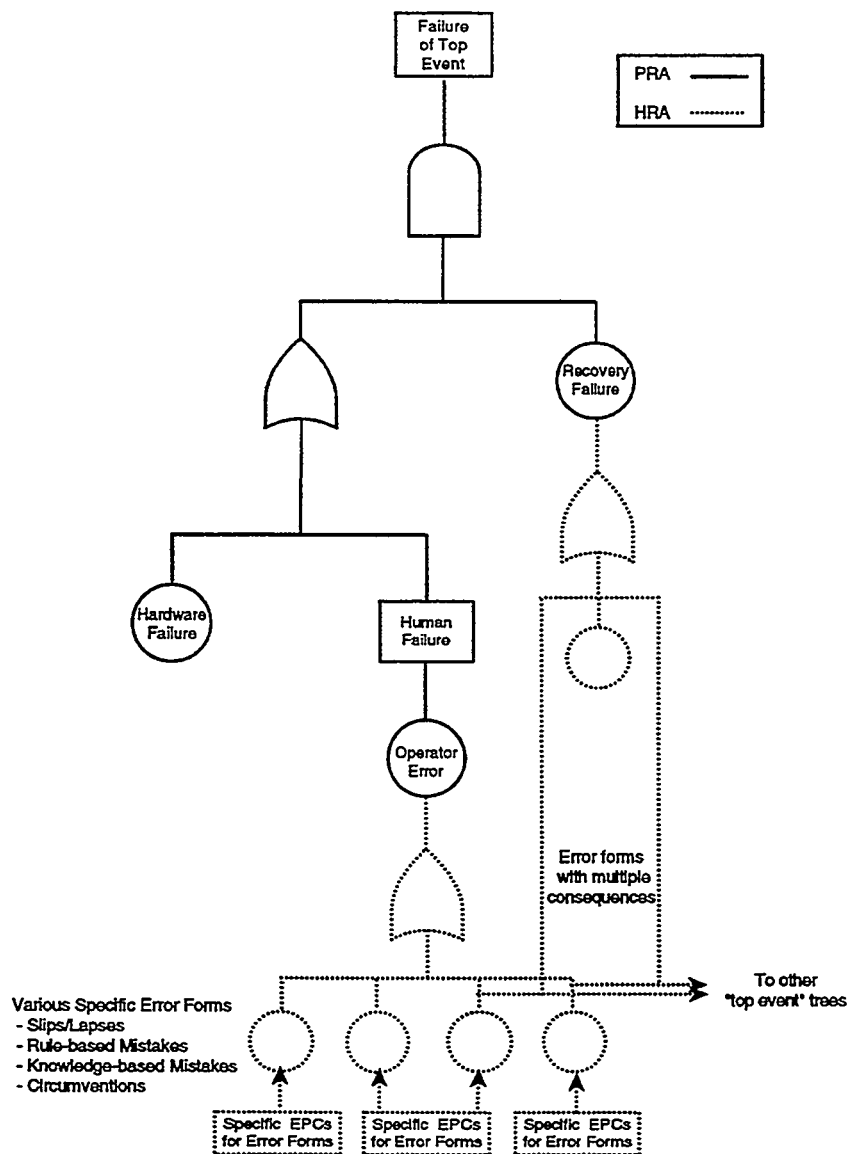
B.2 Existing Frameworks

A limited number of frameworks exist that may be relevant to this work. These are the Rasmussen "stepladder" framework, Reason's GEMS framework, and various representations of decisionmaking from the field of cognitive psychology.
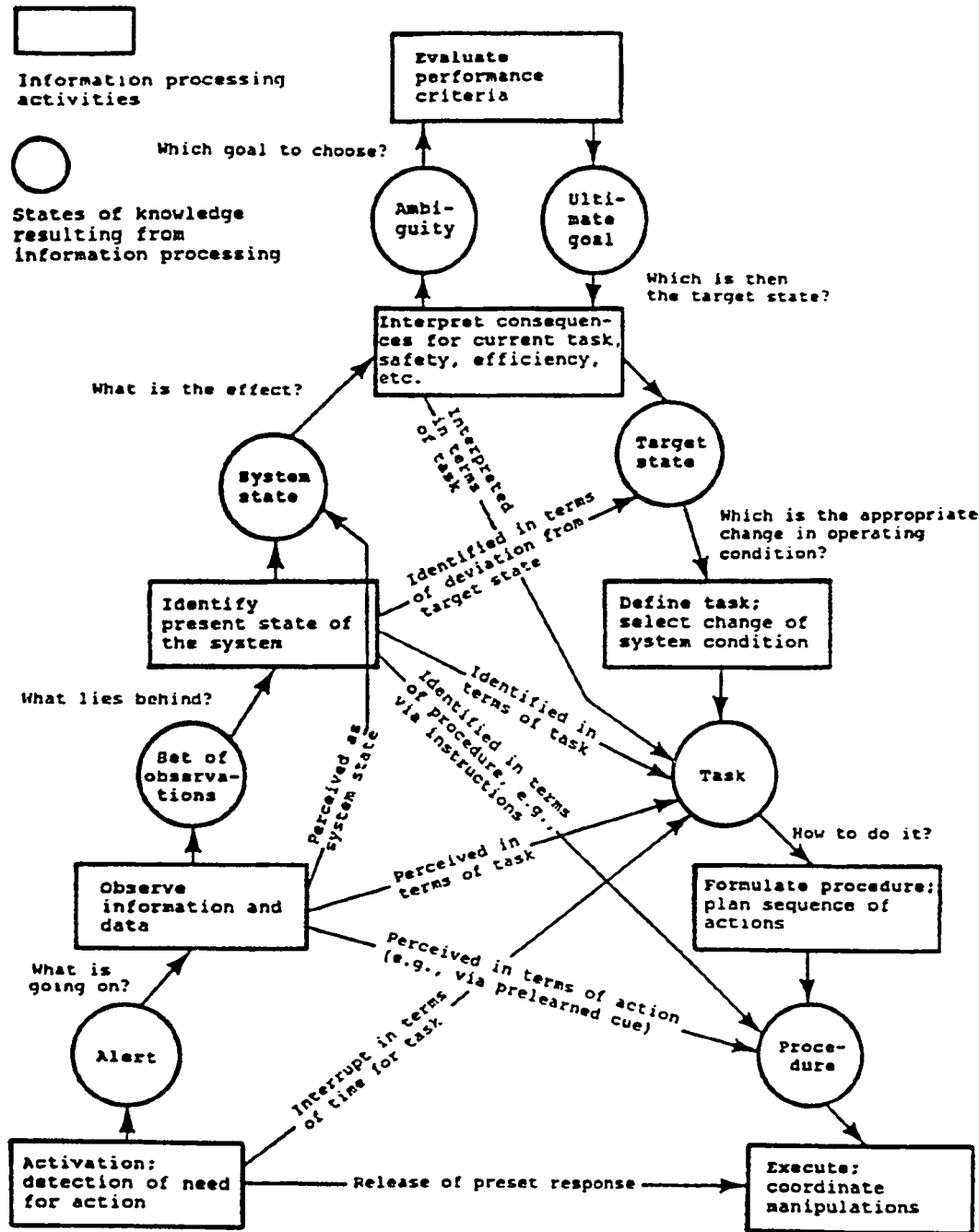
B.2.1 Rasmussen's Stepladder

Rasmussen's stepladder framework[12] is one representation of how humans select action steps from incoming stimuli. It is shown in Figure B.2. Its original purpose was to aid in the development

---

[12]See, for example, Rasmussen, J., "Information Processing & Human-Machine Information: An Approach to Cognitive Engineering," New York: North-Holland, 1986.

Figure B.1. Concept of HRA Construct

Within the figure:

- Failure of Top Event
- PRA ———
- HRA ············
- Recovery Failure
- Hardware Failure
- Human Failure
- Operator Error
- Error forms with multiple consequences
- Various Specific Error Forms
  - Slips/Lapses
  - Rule-based Mistakes
  - Knowledge-based Mistakes
  - Circumventions
- Specific EPCs for Error Forms
- Specific EPCs for Error Forms
- Specific EPCs for Error Forms
- To other "top event" trees

Which goal to choose?

Evaluate
performance
criteria

Ambi-
guity

Ulti-
mate
goal

Which is then
the target state?

Interpret consequen-
ces for current task,
safety, efficiency,
etc.

What is the effect?

System
state

Target
state

Which is the appropriate
change in operating
condition?

Identify
present state of
the system

Define task;
select change of
system condition

What lies behind?

Set of
observa-
tions

Identified in terms of task

Task

Identified in terms of deviation from target state

Identified in terms of task via procedure, e.g., instructions

Observe
information and
data

Perceived as system state

Perceived in terms of task

How to do it?

Formulate procedure;
plan sequence of
actions

What is
going on?

Alert

Perceived in terms of action
(e.g., via prelearned cue)

Interrupt in terms of time for task

Proce-
dure

Activation;
detection of need
for action

Release of preset response

Execute;
coordinate
manipulations

Schematic map of the sequence of information processes involved in a control decision. Rational, causal reasoning connects the "states of knowledge" in the basic sequence. Stereotyped processes can bypass intermediate stages. Together with the work environment, the decision sequence forms a closed loop. Actions change the state of the environment, which is monitored by the decision maker in the next pass through the decision ladder. [Adapted from Rasmussen (1976) with permission from Plenum Publishing Corp.]

Figure B.2. Rasmussen's "Stepladder" Framework (from [12])

of information technologies (Rasmussen's principal interest) for the spectrum of human activities in industrial settings. It is relatively long-lived, originally having seen the light of day in 1974, and was developed from the analysis of verbal protocols of people trouble-shooting equipment failures. Since then it has become somewhat of an icon for HRA practitioners (much to the chagrin of its creator). However, it does possess some useful characteristics. It does recognize that decisionmaking does not always occur in a single, linear manner. Short cuts can be taken ("skill-based" decisionmaking) based on the frequency of experience and perceived familiarity of evidence and setting. It can be used to describe errors in decisionmaking in terms of particular decision pathways taken "inappropriately." To some degree, it can describe (or at least, suggest) particular kinds of consequential actions that may result from the erroneous decision pathways. For example, a misinterpretation of display data may result in an inappropriate leap from observe to procedure because of similarity of symptoms, when the correct response is observe, to identify, thence to task, and then to procedure. The HRA task would require identification of possible similar symptoms and their frequency (much like the confusion matrix) for that particular failure mode.

Rasmussen has extended his stepladder framework to describe typical error modes in problem solving, as shown in Figure B.3. (The background in this figure is a somewhat simplified form of the stepladder figure, as discussed in [15]). Specific error manifestations would be the local interpretation of these modes. For example, a specific form of "incorrect recall" would depend on specific rules and triggers at the time of the event. The error forms and their underlying modes are discussed in pages 154, et seq., of [15].

B.2.2   Reason's GEMS Framework

Reason's Generic Error-Modelling System (GEMS)[13] is derived largely from Rasmussen's skill-rule-knowledge (SRK) framework associated with the "stepladder" framework described above. It is shown in its schematic form in Figure B.4. However, it is reinterpreted into error modes and classes (slips, lapses, and mistakes) beyond the structure of Figure B.3 above. Like the stepladder framework, it recognizes the diversity of potential decisionmaking errors. Given the SRK basis for GEMS, the framework is extended through the identification the most common error modes, which are listed in Table B.1. These are further discussed in pages 68-94 of [16].

One advantage of this framework is that it based on the observations of error modes and the conditions that produce them, as summarized in the above extract, plus Section 2 of [16]. The second advantage is that the error modes are reasonably well described such that an HRA modeling process could, in principle, be developed from them. One problem is, however, that they are very specific to the particulars of any event such as the immediately prior tasks and their contents. Simply interfacing these details with the much more global specifications of PRA scenarios may prove very difficult.

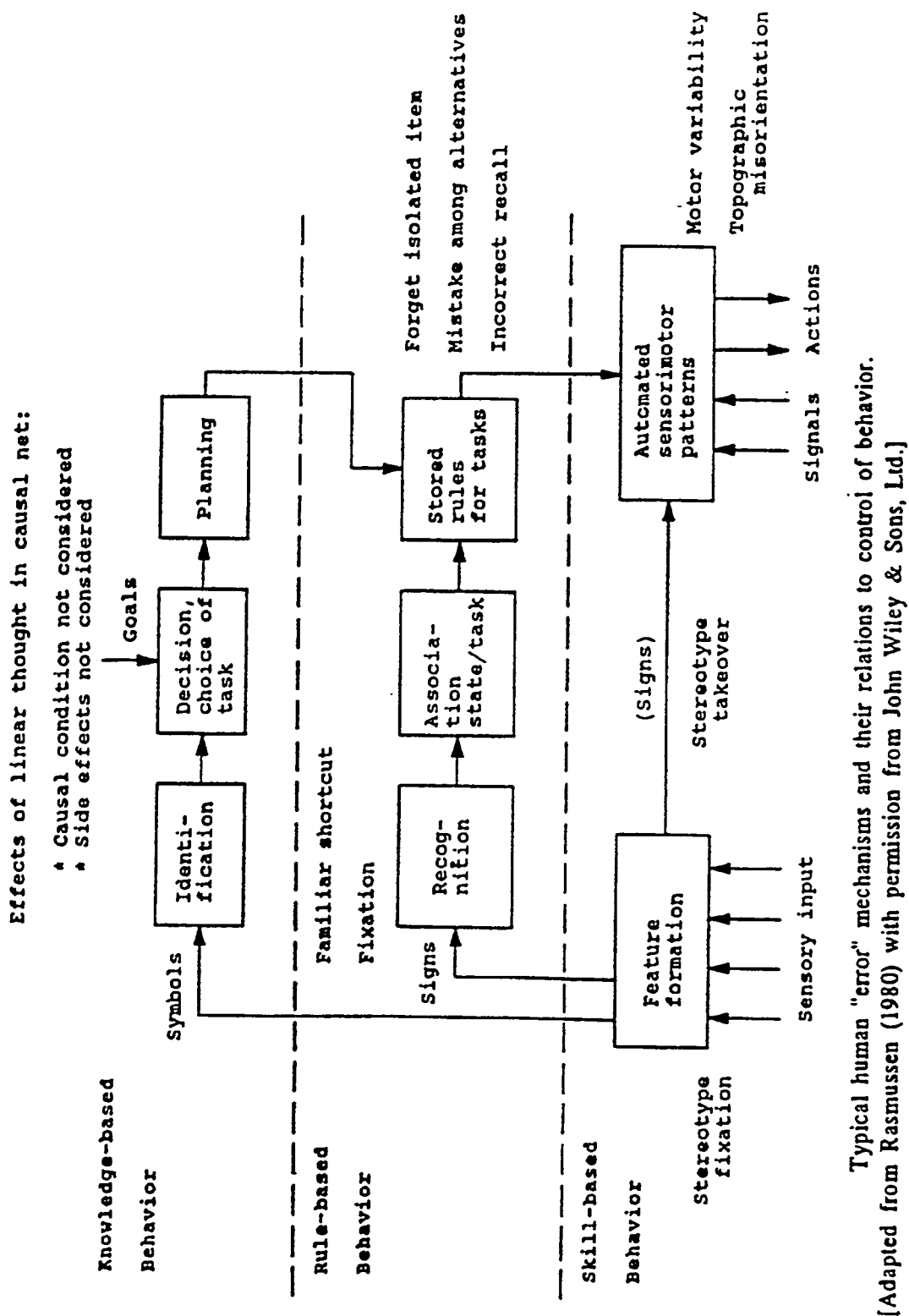[13]Reason, J., "Human Error," New York: Cambridge University Press, 1990.

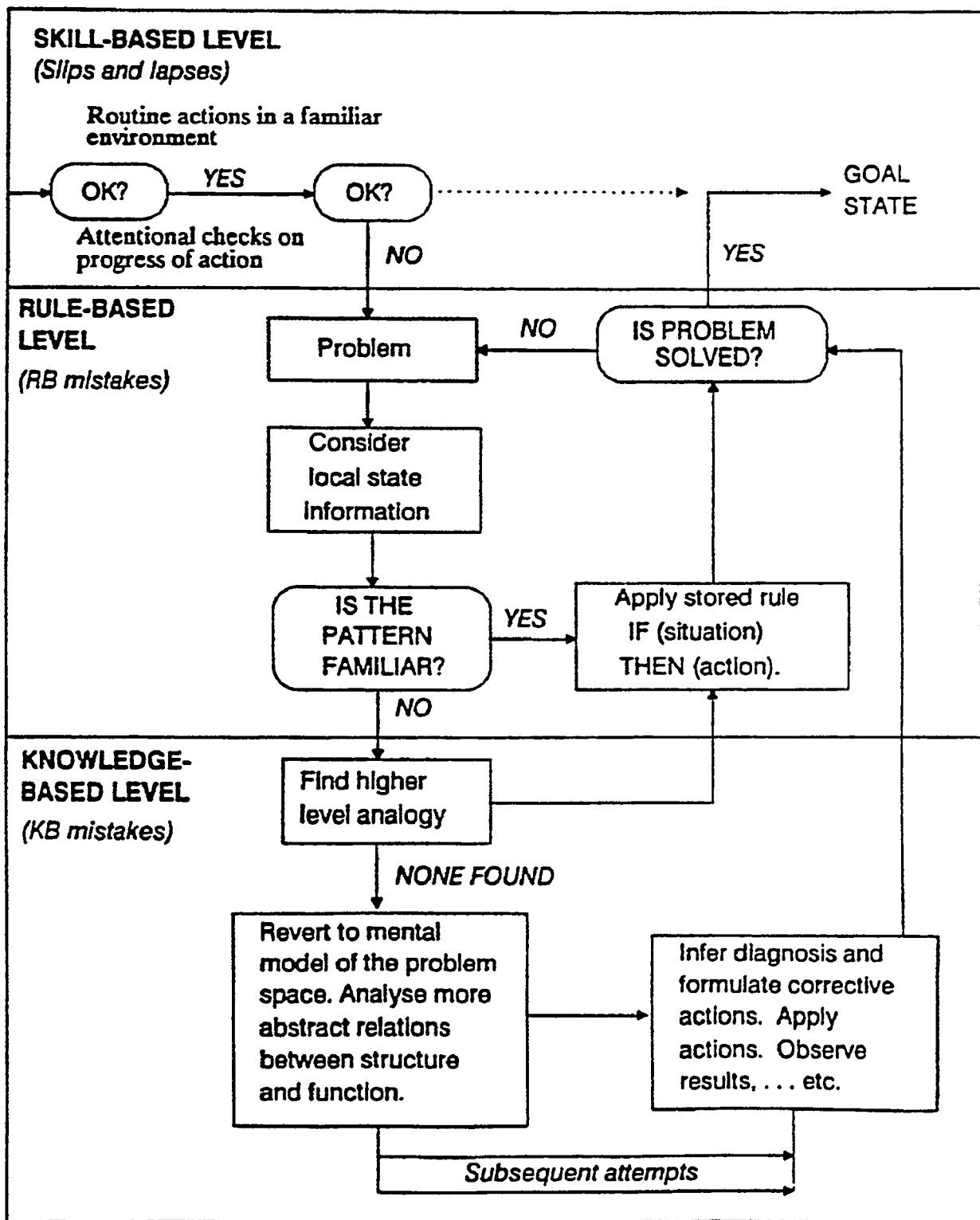**Figure B.3.** "Stepladder" framework with error modes (from [12])

Figure B.4. Generic error modelling systems (from [13])

Table B.1. Common Error Modes (from [13])

Skill-based performance

Inattention	*Overattention*
Double-capture slips	Omissions
Omissions following interruptions	Repetitions
Reduced intentionality	Reversals
Perceptual confusions	
Interference errors	

Rule-based performance

Misapplication of good rules	*Application of bad rules*
First exceptions	Encoding deficiencies
Countersigns and nonsigns	Action deficiencies
Information overload	Wrong rules
Rule strength	Inelegant rules
General rules	Inadvisable rules
Redundancy	
Rigidity	

Knowledge-based performance

Selectivity
Workspace limitations
Out of sight out of mind
Confirmation bias
Overconfidence
Biased reviewing
Illusory correlations
Halo effects
Problems with causality
Problems with complexity
   Problems with delayed feed-back
   Insufficient consideration of processes in time
   Difficulties with exponential developments
   Thinking in causal series not causal nets
   Thematic vagabonding
   Encysting

B.2.3 Resource-Limited Decisionmaker Framework

There are several frameworks developed as part of the world of cognitive psychology to describe decisionmaking activities. One such framework is that implemented in the NRC's Cognitive Environment Simulation (CES) system.[14] The framework is shown in Figure B.5.

In contrast to the earlier frameworks which are taxonomically oriented, CES seeks to provide descriptions of actual decisions using simulation methods--in other words, the specific judgements made for a given decision in a given setting with specific information (procedures, training, and indications). CES establishes decisions based on the interactions of three mechanisms: situation monitors (also called "behavior analysts") identifying abnormal conditions, explanation builders performing the diagnostic functions, and response managers implementing strategies. For example, the actions of a behavior analyst is shown in Figure B.6, taken from [14].

Some effort has been expended in the CES development on creating a set of error processes as important categories of decisions to be simulated; these are summarized on the attached Table B.2, taken from [14].

This framework is built on the concepts of artificial intelligence, and is, in fact, implemented in such a technology using an EAGOL-based AI software system. That in a sense presents a biased view of human behavior. While it is true that people can act like rational problem-solver expert systems, full of "if-then" rules, people possess features not implicit in AI machines: emotions, indolence, curiosity, etc.. To what extent these can be ignored in HRA determines how useful can an AI-based framework be used.

B.2.4 "Bottle-neck" Frameworks

Bottle-neck frameworks come in a variety of guises, but they all derive to a large degree from the single bottle-neck model of Broadbent,[15] developed in 1958 and shown in Figure B.7. This describes the commonly observed features of selective attention and overloading of data processing. Reference [15] presents several variations on this theme.
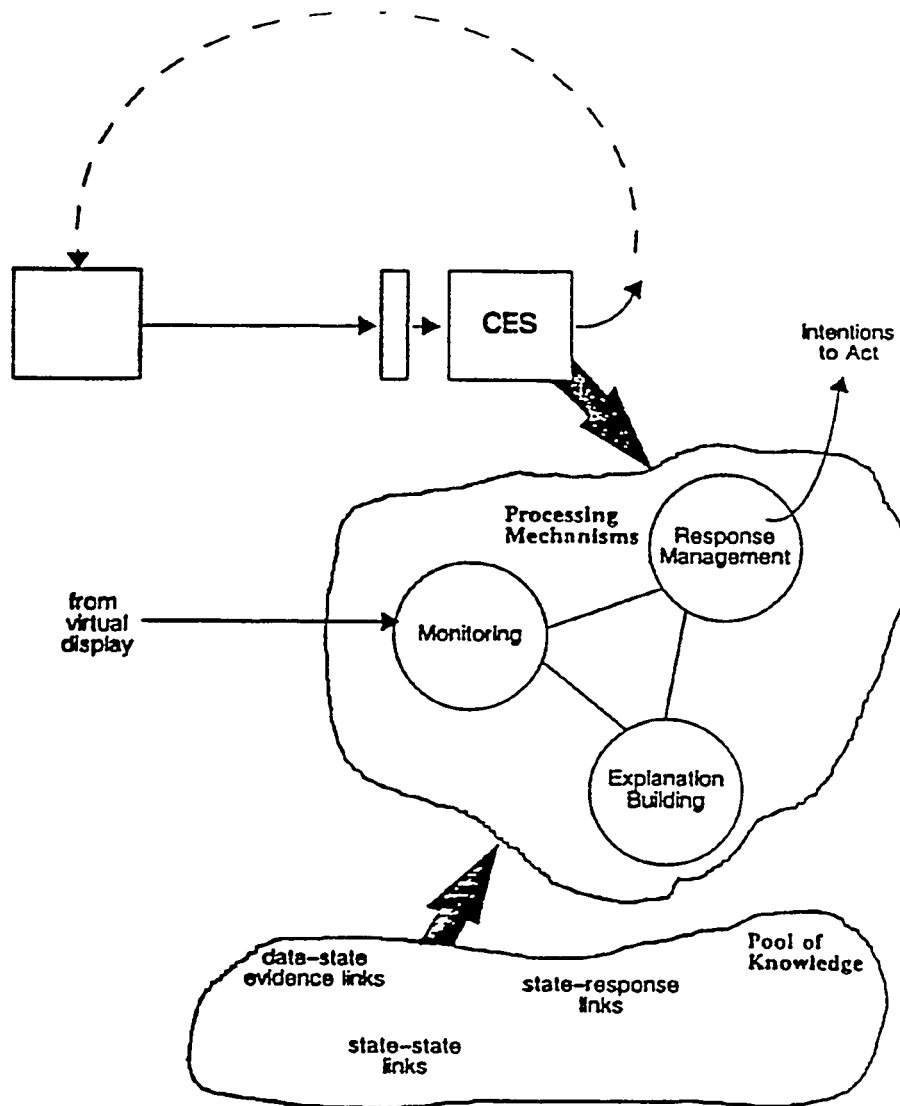
However, as observed by Reason,[16] there are significant limitations in this framework to describe several of the important failure mechanisms such as "strong-but-wrong" that are associated with a "rapid pattern-matching" view of diagnosis. This kind of framework is not seen as ultimately useful for this project but is included for completeness.

---

[14]Woods, D.D., Roth, E.M., and Pople Jr., H., "Cognitive Environment Simulation: An Artificial Intelligence System for Human Performance Assessment," NUREG/CR-4862, Pittsburgh, PA: Westinghouse Electric Corporation, November 1987.
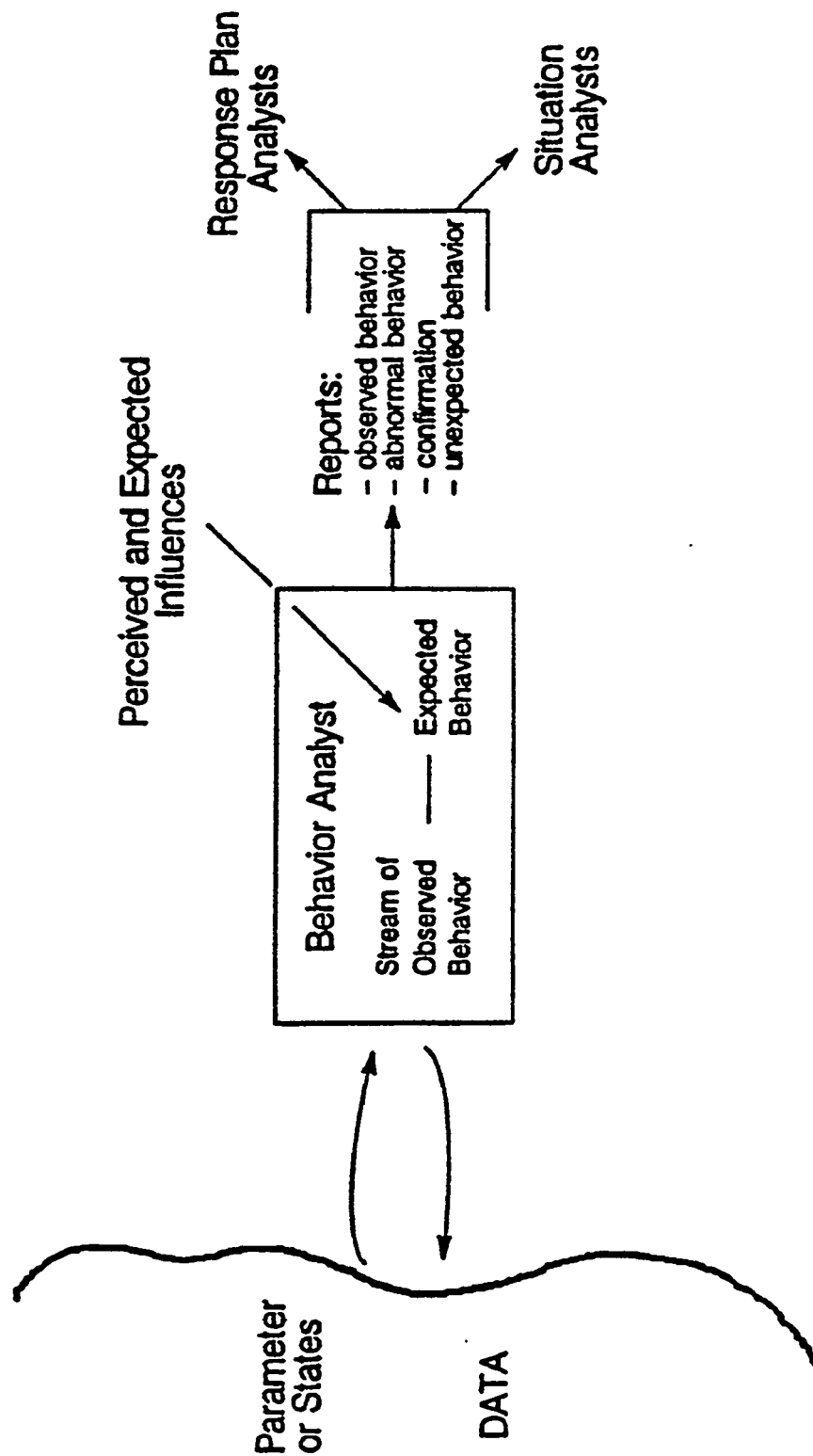
[15]See, for example, Boff, K.R., Kaufman, L., and Thomas, J.P., "Handbook of Perception and Human Performance," Vol. II, New York: Wiley Interscience, 1986, pp. 41-49.

[16]Reason, J., "The Cognitive Worm at the Core of the TRC Model, Panel Session, HRA: Where Goest Thou?," Annual Meeting of the Human Factors Society, Orlando, FL, July 1989.

Figure B.5. CES framework (from [14])

Inside of CES there are different kinds of processing which are carried out "in parallel" so that intermediate results established by one processing activity can be utilized by another and visa versa. This allows a solution to be approached iteratively from different levels of analysis. There are three basic kinds of activities that go on inside of CES: (a) monitoring activities — what parts of the plant are tracked when and are observed plant behaviors interpreted as normal-abnormal or expected-unexpected? (b) explanation building activities — what explanations are considered, in what order, and adopted to account for unexpected findings? (c) response management activities — selecting responses, either expected automatic system or manual operator actions, to correct or cope with observed abnormalities, monitoring to determine if the plans are carried out correctly, and adapting pre-planned responses to unusual circumstances.

Figure B.6. Example of Analysis Used in CES (from [14])

The first processing layer in CES is focused on monitoring of NPP data over time. Associated with each plant parameter state is a behavior analyst who has the responsibility of tracking that parameter. Behavior analysts are not always active. They are created either when a plant parameter or state change meets some criterion (i.e., "data-driven") or when a situation analyst or response plan analyst requires information on the parameter that it is responsible for monitoring (i.e., "knowledge-driven").

Table B.2. Examples of Different Problem Solvers (from [14])

This table contains examples of some emergent patterns of human cognitive processing which are relevant to NPP emergency operations and the settings of CES PAFs which might produce these patterns in CES behavior.

- 1. Vagabond:

  A vagabond problem solver (after Dorner, 1983) abandons the current issue for each new one that arises. The tendency is to jump from issue to issue without satisfactory resolution of any. It is characterized by an incoherent view of the situation and incoherent responses to incidents. This pattern could emerge due to the following, especially when there is some time pressure:

  - failure to synthesize or converge multiple views of the situation,

  - many potential views of the set of significant findings are activated but remain independent,

  - a response orientation emphasized over explanation building so that more coherent explanations never emerge,

  - too interrupt-driven so that every new finding seizes priority.

- 2. Hamlet:

  This type of problem solver looks at each situation from multiple viewpoints and considers many possible explanations of observed findings. However, the result is a tendency to examine possibilities too long before acting because

  - its criterion for judging what is an acceptable explanation is missing or is too general (too many possibilities satisfy it)

  - explanation building is greatly emphasized over response management activities

- 3. Garden Path:

  A garden path or fixation prone problem solver shows excessive persistence on a single issue or activity -- easily fixated, fails to consider revision in face of disprepant evidence. PAFs relevant to produce this type of behavior include:

  - pursues (or is biased to pursue) only a single point of view to explain findings;
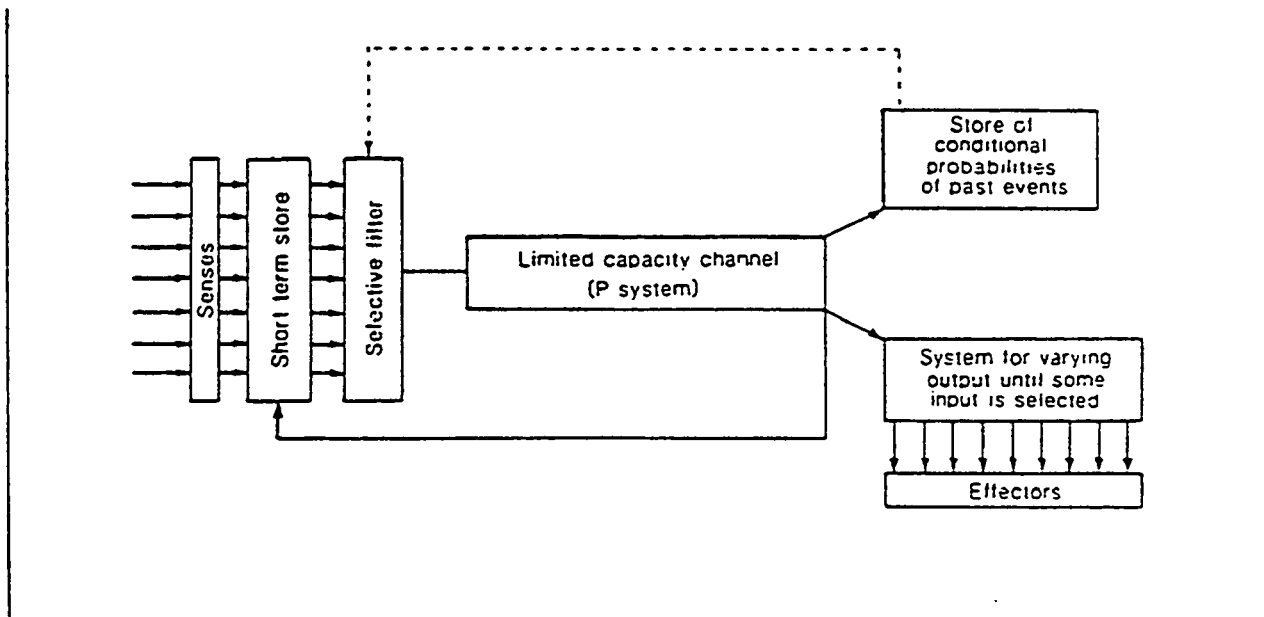
Table 2. Continued

o   not interrupt driven enough; in the extreme case, no new issue interrupts ongoing activity until scheduled activity is completed;

o   insensitive to violations of expectation, after an initial explanation is accepted, because too narrow a field of view or because response management overrides explanation building.

● 4. Inspector Plodder:

This type of problem solver slowly and deliberately builds up and then narrows in on possibilities. It exhibits very thorough consideration of evidence and possible explanations via explicit consideration of evidence and possible explanations via explicit chains of reasoning (minimal reasoning shortcuts). The result is good, thorough, but slow problem-solving. Performance adjustment factors related to thispattern are a narrow field of attention; low interruptability; sequential, deep exploration of possible explanations, good criteria for scheduling competing activities, and good criteria for what is a good explanation.

● 5. Expert Focuser:

This problem solver is adept at seeing and focusing in on critical data for the current context so that it is always working on the most relevant part of the situation. The whole situation tends to fall quickly into place, and revisions are easily made when appropriate. Performance adjustment factors related to this pattern are a wide field of attention; high level of interruptability; good criteria for scheduling competing activities; good criteria for what is a good explanation.

A diagram of the flow of information within the nervous system. Information received by the senses is transmitted in parallel to the short-term buffer and arrives at the filter. The filter is tuned to pass only messages having relevant physical properties, one message at a time, to the central processor. The central processor precedes the long-term store and the response mechanisms. The filter protects the central processor from overload. Screening of information is done at an early stage, before semantic analysis (the costly operation) has been performed. (From D. E. Broadbent, *Perception and communication*. Copyright 1958 by Pergamon Press. Reprinted with permission.)

Figure B.7. "Bottleneck" framework (from [15])

B.2.5 Selection of Framework

Of the existing constructs that describe errors in decisionmaking, GEMS has the greatest potential for use in the development of a new class of human reliability models. It has the greatest potential because the descriptions of error modes can be related to two key requirements for integration with the needs of the PRA users. First, different error modes can lead to different consequences in terms of the PRA/HRA interface. For example, mistakes (errors of intention) are much more likely than slips to result in multiple dependent human failure events in accident sequences. Second, the supporting discussion in [16] provides a basis for considering specific shaping factors for the different error modes. Such guidance could be used as one input to the data-analysis task, as discussed below.

B.3   Example Use of Construct

Using Reason's GEMS framework and the associated principal error modes, it is, in principle, possible to take specific error modes and relate them to the activities during LP/SD operations, to identify possible specific types of failures that are associated with PRA issues. For example, take a failure event in PRA space, operator terminates operation of pump "x" at an inappropriate time. The procedure would work somewhat in the following fashion. Figure B.8 indicates the possible process for the major activities.

1.   What error types reasonably could be expected to lead operators to perform that erroneous act? For example, which error types associated with inattention or overattention could be seen as leading to performing that act? Which error types associated with misapplication of good rules or application of bad rules? Ditto, the knowledge-based types.

2.   What kinds of error types considered in 1. were identified in the HACS reviews? If rule-based error types seemed to predominate the above kinds of failures (for example), were there common patterns of such types across several events?

3.   If some patterns emerged in 2., then can the various PSFs associated for these significant error types can be sought (based on the discussions in pp. 68-96 of Human Error)? The intent is to limit the consideration of error types to only the most significant.

4.   The PSFs should be expressed (or reinterpreted) in terms of potentially observable and auditable factors that could be evaluated prospectively in future PRA contexts; see Section 4.2 below.

5.   The HRA/PRA interface should be at the level of the PRA identifying the specific failures that are to be incorporated in the systems models, using (perhaps) a classification scheme of activities jointly developed between HRA and PRA practitioners. The HRA analysts then develop a description of the most risk-significant potential failure modes (a check-list will do) that ranks mistakes as potentially having the most severe consequences, then unrecoverable slips & lapses, and finally recoverable slips & lapses. One HRA judgement is to consider the relative frequencies to assign the relative risk potentials. Based on these, the associated PSFs (4. above) need to be assessed for the most significant error modes.

Figure B.8. Potential Evaluation Process

B.4   Implications for Other Tasks

Based on the above outline of an methodology, several implications arise for other tasks.

B.4.1   Systems Modeling Tasks (Tasks 4.1 and 4.2)

Tasks 4.1 (Identify and Represent Errors of Commission) and 4.2 (Approach to Deal with Dependency) involve the development of interfaces between the HRA and PRA technologies to develop means for representing the opportunities and consequences of "errors of commission" and other types of dependent consequences. The methods developed in these tasks will be influenced strongly by the construct developed in Task 3. Specifically the different kinds of error modes identified in the construct will require rules to be developed for how to identify the multiple dependent failures consequential on the occurrence of particular error modes. For example, the multiple consequences of a mistake involving misdiagnosis would be the actions taken in accordance with the procedures corresponding to the mistaken diagnosis. These multiple actions would need to be examined to identify which have the effect of changing significantly the accident sequences as modelled. Other error modes would be examined to identify the potential dependent consequences.

B.4.2   Quantification (Task 4.3)

The primary source of data for HRA quantification is expected to be through expert opinion. There are simply no data sources known that can provide data for the spectrum of error modes and consequences required in these methods.

Such data will require particular data-gathering methods involving estimation of PSFs at the error-mode level. For example, one error mode found important in the data survey was errors contained in procedures, which led to mistakes. The data for this error mode are the conditional probabilities that a procedure contains technical errors of such a significance as to increase the likelihood of a consequence of concern in the PRA. The data-gathering task should be able to obtain data associated with this specific mode by considering what are the most important factors in allowing such failures, and how can they be assessed by observable evidence. By limiting the consideration of the number of error modes, only a moderate number of such data assessments be required.

Appendix C. An Approach to the Development of the Quantification Methodology

C.1 Step 1. Establish a "Strawman" Taxonomy of Factors and Subfactors Influencing Error Expressions

Before proceeding to elicit information from operational and systems experts, the "in-house" expertise of the project team will be used to develop a strawman taxonomy. The project team includes expertise in HRA, PRA, nuclear systems and nuclear operations, as well as behavioral science. This development includes an initial attempt to structure the factors in a way that is consistent with the behavioral construct discussed in Task 3. For example, it will include an initial attempt to identify groupings of factors that are expected to be more important for slips vs. mistakes. HACS, developed during Phase 1 of this study, will be a starting point for development of the taxonomy. Particular consideration will be given to the root cause analysis taxonomy from HPIP, which was incorporated into HACS. The HPIP categories of causal factors were intended to be very much operationally oriented.

C.2 Step 2. Identify Important Influence Factors, Relationships Among Factors, and Causal Relationships Between Factors and Error Expressions

Using in-depth interview techniques, with a small number of experts, identify the important factors influencing human error in nuclear plant operations, and extract expert strategies for determining the impact that variations in causal factors have on performance. This will be accomplished by first identifying from PRA studies and actual events a set of sequences, plant systems, human actions and error expressions which can be used to provide a context for the experts to work with. These "sample performances" will be selected to be representative of a range of systems, types of errors, and other critical dimensions. The sample performances then will used to elicit from the experts the factors and relationships of interest. In the context of specific situations experts are more readily able to express their implicit strategies for evaluating the factors of importance.

This process will be initiated by using experts within the project team and then refining their input by going through the same processes with external subject matter experts. The external experts add robustness and serve as an initial "validation" of the judgment of the team's experts. The elicitation process to be used will extract both qualitative information about the factors and their interrelationships, and *relative* quantitative relationships. Experts will not be asked to judge absolute values of human error probabilities, and certainly not out of the context of realistic sample performances.

A number of different techniques exist to anchor the relative judgments relatively well established numerical values. A technique that will be explored for use, which is much more consistent with the basic intent of exploration of human behavior *in context*, is to "seed" the sample performances with items that are readily quantifiable by the expert, and have the expert compare relative estimates of human reliability to the seeded value. For example, experts are expected to be very familiar with certain equipment failure rates, sample performances involving that equipment could be used in the interviews, and experts could compare estimated human reliabilities to those equipment reliabilities. The point is to provide experts a basis of comparison from within their own experience. Elicitation through in-depth analysis with a small number of experts will identify major differences in strategies and viewpoints. These differences offer rich insights into the reasons for variations in performances. A consensus of a large number of experts is not a goal of this approach, and traditional consensus techniques will not be used.

C.3 Step 3. Synthesize a Mathematical Model Relating Causal Factors to Error Expressions

At the simplest level, this task might consist of simply rank ordering various cases of error expression and "anchoring" the scales with some well identified or agreed upon values. The approach proposed is to use software developed by Connelly[17] to perform scaling, ranking and preference modeling. This software will assist in

producing, or "synthesizing," mathematical models which produce quantitative estimates that consistently and reliably reproduce the results that the experts predict. The complete model will include (1) a set of "rules" for the user to assess the various causal factors in his own system, (2) guidance for selection of quantitative parameter values to input into the model, and (3) the mechanisms for calculating performance (e.g., equations, graphs, tables).

C.4 Step 4. Evaluate and Refine the Mathematical Model

Available and practical strategies for evaluating the effectiveness of the model will be applied, including comparison of results of different evaluators (independent of the original contributors), comparison with results of other methodologies, and comparison with available data.

C.5 Step 5. Data Collection and Analysis in Support of Development

In support of, and interactive with, the development of the quantitative approach this task will continue and expand the effort initiated during Phase 1 of the project to collect and assess data from actual operating experience. This effort will provide input to the development of the approach as well as an alternate source of information for external "validation" of results.

---

[17]Connelly, E.M., "The Theory of Human Performance Assessment," Proceedings of the Human Factors Society, 1987.

APPENDIX E

INTERVIEW PROTOCOLS

INTERVIEW GUIDE
HUMAN PERFORMANCE AND SAFETY DURING
LOW POWER AND SHUTDOWN (LP&S) OPERATIONS
UTILITY PERSONNEL

INTERVIEWEE:

    Utility: _____

    Name: _____

    Position:

INTERVIEWERS: _____

                         _____

                         _____

DATE: _____

INTRODUCTION

USNRC, through BNL and SNL, is studying the issue of human performance and its contribution to safety during low power and shutdown (LP&S) operations. Several events at operating reactors suggest that more emphasis may need to be placed on safety in these phases of plant operation. Preliminary reviews by NRC staff and by the national laboratories indicate that human performance has played a significant role in the initiation and/or response to these events. The purpose of this interview is to obtain your input regarding safety related human performance during LP&S operation. We will try to do this by asking questions in three general areas: (1) general information about LP&S operations focused on safety functions and critical human tasks related to safety; (2) the factors that contribute to good performance or human error during one or more of those critical tasks; and, (3) one or more specific examples from your experience of incidents that illustrate significant safety issues in LP&S operation, in particular ones that illustrate issues of human performance in LP&S operation. The questions in this guide are used simply to stimulate discussion. Any input you have is important. Please interrupt, pass on any questions you don't care to answer, and freely address what you think are the important issues. Any questions?

PART I: GENERAL INFORMATION, LP&S OPERATIONS

1.   With regard to potential impact on safety, what do you think are the most important factors that differ between LP&S and normal operations? Examples might be differences in staffing, roles and responsibilities, availability of safety related equipment, workload and schedule demands, administrative controls, procedures, training, tech specs, etc. For each factor identified, explain the major differences and how those differences might impact safety.

2.   What are the critical safety functions specified in your EOPs?

3.   What are the major plant conditions or configurations your plant goes through during LP&S operations? A listing of Plant Operating States (POSs) identified by NRC is attached for reference/comparison.

4.   Considering these plant conditions and the critical safety functions, what do you consider the activities, operations, or situations that present the greatest challenges to maintaining the safety functions during LP&S operations?

5.   For each of the activities/situations identified in Question 4 as a challenge to safety during LP&S, what are the human actions - tasks or groups of tasks - that are especially noteworthy because of their importance to maintaining a critical safety function, because they are especially complex or difficult, or in some other way are "critical" human actions?

6.   What do you consider to be the important factors that distinguish a good shutdown (outage) management program? How would you know a good one (or poor one) if you saw it?

7.   If you were called in to evaluate safety performance in an ongoing outage, how would you know whether or not the outage was being conducted safely? Especially with regard to human performance, what would you look for to identify safe or unsafe performance?

8.   What special measures are taken in your plant to assure protection of critical safety functions during LP&S operations (e.g., administrative controls, physical barriers to protect sensitive equipment, outage training)?

9.   If an incident or error does occur, how is the appropriate corrective action determined? What determines whether or not a root cause analysis is performed and what level/type of corrective action is needed?

PART II: CRITICAL TASK INFORMATION

Considering a few of the most important human actions identified in Question 5 above, provide for each action as you can the following:

1.   A brief label/description of the human action.

2.   What is the plant operating state (POS) during which the human action occurs?

3.   Who (job position) performs the human action?

4.   What is the purpose/intent of the human action?

5.   What is the general activity/situation - maintenance/repair, testing, response to off-normal condition, etc.

6.   General location - control room, outage control area, refueling floor, etc.?

7.   How frequently is this action performed during LP&S?

8.   What is the "initiator" for the human action - procedure, supervisor instruction, alarm, etc.

9.   Important human performance requirements, e.g., time-critical task, must be done very precisely, requires extensive knowledge of system operation,.

10.   Any tools, aids, special resources required?

11.   Communications, coordination, interfaces with other persons required?

12.   System feedback - what indications are there from instrumentation, system response, supervisor review, etc. that provide feedback to the human about the success/failure of the action taken? Note both the quality and timeliness of the feedback.

13.   Plausible error modes - what are the most likely ways that a human error could occur?

14. Of the many factors that might influence human performance/error, several categories are listed below. Please rate each of these as low, medium or high importance as a potential contributor to human performance for this critical action:

FACTOR	(CIRCLE ANSWER)		
Procedures	LOW	MEDIUM	HIGH
Training	LOW	MEDIUM	HIGH
Communications	LOW	MEDIUM	HIGH
Organizational Factors	LOW	MEDIUM	HIGH
Human Engineering	LOW	MEDIUM	HIGH
Supervision	LOW	MEDIUM	HIGH
Stress	LOW	MEDIUM	HIGH
Engineering Changes	LOW	MEDIUM	HIGH

Other (list as many as
desired below and rate them)

Please discuss why these factors do or do not influence the specific human action discussed above.

15. Impact of human error. In this critical task, what could be the ultimate (worst-case) impact of the human error- on plant equipment, safety, etc. - if the human error were not recognized and corrected? If the worst-case would require additional equipment/human failures, try to identify those additional failures. What is the most likely impact?

16. Recovery - how would the human error be discovered and corrected? How likely is this recovery to occur before the "ultimate" impact described above would occur?

17. Ideally, what could be done to correct or improve the factors that contribute to error or prevent the error?

NUREG/CR-6093

PART III: CRITICAL INCIDENT ANALYSIS

Have you ever experienced a situation during LP&S in which there were important human errors, near misses, or perhaps extraordinarily effective human performance? (If not, focus the interviewee's attention on a "hypothetical" example of an important occurrence, or one with which he/she is familiar from discussions with others.) Focusing on each "critical incident" one at a time, address the following for each incident (interviewer should have additional copies ready):

1.   What was the situation surrounding the human action? Plant state, activity in progress, related conditions, equipment failures, abnormal event, etc. Was there anything unusual for your plant (compared to typical LP&S operations). For example, was there equipment out of service that is normally operating during LP&S?

2.   What was the specific human action involved, and what was the error or exceptional performance?

3.   What was the impact or potential impact of the human action?

4.   What were the important causes or contributing factors associated with the human action? Did the plant perform any root cause investigation of the human performance involved? If so, what were the findings?

5.   How was the error discovered? Corrected?

6.   How frequently does this situation arise in LP&S and how likely is the specific human error (or exceptionally effective performance) given that the situation does occur?

**INTERVIEW GUIDE
HUMAN PERFORMANCE & SAFETY DURING
LOW POWER & SHUTDOWN (LP&S) OPERATIONS
NON-UTILITY PERSONNEL**

<u>INTERVIEWEE:</u>

    Organization: _____

    Name: _____

    Position: _____

<u>INTERVIEWERS:</u> _____

                                  _____

<u>Date:</u> _____

Q1: As part of your work, what aspects of human performance or low power operations have you been studying? Are there any particular characteristics or issues that you have been focussing on in this work (e.g., procedures, equipment, availability, training)?

Q2: What products, e.g., reports, guidelines, or data sources, have you or your organization produced related to the assessment, enhancement, or quantification of human performance in LP&S?

Q3: What do you believe are the most important lessons to be learned from your review of LP&S activities?

Q4: Within your area of analysis, what seem to be the most important characteristics of LP&S operations that influence the level of safety?

    a. Plant activities or conditions (e.g., fuel movement, reduction in RCS inventory, maintenance/installation of new equipment concurrent with plant activities, decay heat removal, presence of many contractor staff)? Are any of the plant activities or conditions unique to PWRs (vendors) or BWRs (type/Mark)?

    b. Human Performance - Of the many factors that might influence human performance/error, several categories are listed below. Please rate each of these as low, medium, or high importance as a potential contributor to human performance.

FACTOR	CIRCLE ANSWER		
Procedures	Low	Medium	High
Training	Low	Medium	High
Communications	Low	Medium	High
Organizational Factors	Low	Medium	High
Human Engineering	Low	Medium	High
Supervision	Low	Medium	High
Stress	Low	Medium	High
Engineering Changes	Low	Medium	High
Other	Low	Medium	High

(list as many as desired below & rate)

Q4: (Continued)

    b. (continued)

Please discuss in more detail any of the above factors as you wish and indicate how they differ during LP&S as compared to normal operations.

Q5: What do you consider to be the important factors that distinguish a good shutdown (outage) management program? How would you know a food one (or poor one) if you saw it? (If answers are not forthcoming, examples of characteristics might be suggested as follows from NUMARC 91-06 guidance; namely, the enclosed mentioned key elements of outage planning and control: Integrated Management, Level of Activities, Defense in-depth, Contingency Planning, Training, and Outage Safety Review).

Q6: What observables in the plant are there that distinguish a good outage from a poor one in particular with regard to safety (e.g., barrier or warning sign versus lack thereof)? If you were called in to evaluate safety performance in an ongoing outage, how would you know whether or not the outage was being conducted safely? Especially with regard to human performance, what would you look for to identify safety or unsafe performance?

Eric Beckjord
USNRC-RES/DO
MS: T-10F12

Robert Bernero
USNRC-NMSS/DO
MS: T-8A23

Andrea Besi
Institute for Systems Engineering
  and Informatics
CEC Joint Research Centre
CP N 1
1-21020 Ispra (Varese)
ITALY

John Bickel
Idaho National Engineering Lab.
EG&G MS: 3850
P.O. Box 1625
Idaho Falls, ID 83415

Vicki Bier
Dept. of Industrial Engineering
University of Wisconsin-Madison
1513 University Avenue, Room 389
Wisconsin, WI 53706

Scott Bigelow
S-CUBED
2501 Yale SE, Suite 300
Albuquerque, NM 87106

Prof. Dr. Dr.-Ing. E. H. Adolf
  Birkhofer
Gesellschaft für Anlagen und
Reaktorsicherheit (GRS) mbH
  Forschungsgelände
D-8046 Garching
Federal Republic of Germany

David Black
American Electric Power
1 Riverside Plaza
Columbus, OH 43215

Harold Blackman
Idaho National Engineering Lab.
EG&G MS: 3850
P.O. Box 1625
Idaho Falls, ID 83415-3850

Dennis Bley
Buttonwood Consulting
17291 Buttonwood St.
Fountain Valley, CA 92708

Roger Blond
Booz-Allen & Hamilton
4330 East West Highway
Bethesda, MD 20814

M. P. Bohn
Division 6449
Sandia National Laboratories
Albuquerque, NM 87185

Dr. Mario Bonaca
Manager, Reactor Engineering
Northeast Utilities
P.O. Box 270
Hartford, Conn. 06141

Robert B. Borsum
Nuclear Power Division
B & W Nuclear Tech
1700 Rockville Pike
Suite 525
Rockville, MD 20852

Stephen Boult
Electrowatt Engineering Services
  (UK) Ltd.
Grandford House
16 Carfax, Horsham
West. Sussex RH12 IUP
ENGLAND

Gary Boyd
Safety & Reliability Optimization
  Services
9724 Kingston Pike, Suite 102
Knoxville, TN 37922

Brookhaven National Laboratory (2)
Attn: Lev Neymotin
      Arthur Tingle
Building 130
Upton, NY 11973

David M. Brown
Paul C. Rizzo Associates, Inc.
300 Oxford Drive
Monroeville, PA 15146-2347

Tom D. Brown
Sandia National Laboratories
Dept. 6413
P.O. Box 5800
Albuquerque, NM 87185

Robert J. Budnitz
Future Resources Associates, Inc.
2039 Shattuck Avenue, Suite 402
Berkeley, CA 94704

Gary Burdick
USNRC-RES/SAIB
MS: T-10F13

Arthur Buslik
USNRC-RES/PRAB
MS: T-9F31

Edward Butcher
USNRC-NRR/SPSB
MS: O-10E4

Technical Library
B&W Nuclear Service Co
P. O. Box 10935
Lynchburg, VA 24506

Stefaan Caeymaex
Safety & Systems Section
Nuclear Generation Dept.
TRACTEBEL
Avenue Ariane 7
B-1200 Bruxelles
BELGIUM

Leonard Callan, Administrator
U.S. Nuclear Regulatory Commission
Harris Tower and Pavilion
611 Ryan Plaza Drive, Suite 400
Arlington, TX 76011-8064

J. Calvo
Division of PSA & Human Factors
Consejo de Seguridad Nuclear
Calle Justo Dorado, 11
28040 Madrid
SPAIN

A. L. Camp
Division 6412
MS: 0748
Sandia National Laboratories
Albuquerque, NM 87185-0748

John Forbes Campbel
HM Superintending Inspector
Health & Safety Executive
St. Peter's House
Balliol Road
Bootle L20 31Z
UNITED KINGDOM

Leonel Canelas
New University of Lisbon
Quinta de Torre
2825 Monte de Caparica
PORTUGAL

Harold Careway
General Electric Co., M/C 754
175 Curtner Ave.
San Jose, CA 95129

D. D. Carlson
Division 6411
Sandia National Laboratories
Albuquerque, NM 87185

Jose E. De Carlos
CSN International Coordinator
Consejo de Seguridad Nuclear
Calle Justo Dorado 11
28040 Madrid
SPAIN

Annick Carnino
International Atomic Energy Agency
Wagramerstrasse 5, P.O. Box 100
A-1400 Vienna
AUSTRIA

S. Chakraborty
Swiss Federal Nuclear Safety
   Inspectorate
Hauptabteilung für die Sicherheit
   der Kernanlagen
CH-5232 Villigen-HSK
SWITZERLAND

Erulappa Chelliah
USNRC-RES/PRAB
MS: T-9F31

Mike Cheok
NUS
910 Clopper Road
Gaithersburg, MD 20878

Nilesh Chokshi
USNRC-RES/SSEB
MS: T-10L1

T. L. Chu
Brookhaven National Laboratory
Department of Nuclear Energy
Bldg. 130
Upton, NY 11973

Peter Cooper
SRD/AEA Technology
Wigshaw Lane
Culcheth
Cheshire   WA3 4NE
England

Susan E. Cooper
Science Applications Int'l. Corp.
11251 Roger Bacon Drive
Reston, VA   22090

Michael Corradini
University of Wisconsin
1500 Johnson Drive
Madison, WI 53706

E.R. Corran
ANSTO Reasearch Establishment
Lucas Heights Reserch Labs.
Private Mail Bag 1
Manai, NSW 2234
AUSTRALIA

Massimo Cozzone
A.N.P.A.
Via V. Brancati, 48
I-00144 Rome
ITALY

George Crane
1570 E. Hobble Creek Dr.
Springville, Utah 84663

Mark Cunningham
USNRC-RES/PRAB
MS: T-9F31

S. Daggupaty
Environment Canada
4905 Dufferin Street
Downsview
Ontario, M3H ST4
CANADA

Louise Dahlerup
Inspectorate of Nuclear Inst.
Danish Civil Defense &
  Emergency Planning Agency
16, Datavej
DK-3460 Birkerod
DENMARK

John Darby
SEA, Inc.
6100 Uptown Blvd. NE
Albuquerque, NM 87110

Gerald Davidson
Fauske and Associates, Inc.
16 W 070 West 83rd Street
Burr Ridge, IL 60521

Peter Davis
PRD Consulting
P.O. Box 2046
Sheridan, WY 82801

P. De Gelder
Secretary, BELGIAN NUCLEAR
  SOCIETY (BNS)
A V Nuclear
Avenue du Roi 157
B-1060 Brussels
BELGIUM

Lennart Devell
Studsvik Nuclear
Studsvik Energiteknik AB
S-611 82 Nykoping
SWEDEN

J. Devooght
Service de la Metrologie Nucl
University Libre de Bruxelles
Faculte des Sciees Appliqu.
50 Avenue F-D Roosevelt
Bruxelles 5
BELGIUM

G. Diederick
Commonwealth Edison Co.
LaSalle County Station
RR1, Box 220
2601 North 21st Rd.
Marsielles, IL 61341

Chuck Dobbe
Idaho National Engineering Lab.
EG&G MS: 3840
P.O. Box 1625
Idaho Falls, ID 83415

Mary Drouin
USNRC-RES\SAIB
MS: T-10F13

Duke Power Co. (2)
   Attn: Duncan Brewer
         Steve Deskevich
422 South Church Street
Charlotte, NC 28242

Bill Eakin
Northeast Utilities
Box 270
Hartford, CT 06141

Stewart D. Ebneter
USNRC
101 Marietta St., Suite 2900
Atlanta, GA 30323-0199

Adel A. El-Bassioni
USNRC-NRR/PRAB
MS: O-10E4

ENEA/DISP (2)
Attn: Alvaro Valeri
      Alfredo Bottino
Via Vitaliano Brancati, 48
00144 Roma EUR
ITALY

Walter P. Engel
PRAG MGR Analysis & Reg Matter
NE-60
CRYCITY
US DOE
Washington, DC 20585

John Flack
USNRC-RES/SAIB
MS: T-10F13

Karl Fleming
Pickard, Lowe & Garrick
2260 University Drive
Newport Beach, CA 92660

Terry Foppe
Safety Analysis Engineering
Rocky Flats Plant
Energy Systems Group
Rockwell International Corp
P.O. Box 464
Golden, CO 80401

R H. Gauger
Manager-Reliability Engr
A/E Div
Holmes & Narver Inc.
R Roanne Circle
Irvine, CA 92714

Robert Gobel
Clark University
Center for Technology, Environment
   and Development
950 Main St.
Worcester, MA 01610-1477

Paul Govaerts
Studiecentrum voor Kernenergie
(SCK/CEN)
Boeretang, 200
B-2400 Mol
BELGIUM

Mr. Gubler
International Atomic Energy Agency
NENS/SAD BO842
Wagramerstrasse 5, P.O. Box 100
A-1140 Vienna
AUSTRIA

Paul M. Haas, President
Concord Associates, Inc.
725 Pellissippi Parkway
Suite 101, Box 6
Knoxville, TN 37933

F. T. Harper
Division 6413
MS: 0748
Sandia National Laboratories
Albuquerque, NM 87185-0748

Dr. U. Hauptmanns
Gesellschaft Für Anlagen und
  Reaktorsicherheit (GRS) mgH
Schwertnergasse 1
D-5000 Köln 1
GERMANY

Sharif Heger
UNM Chemical and Nuclear
  Engineering Department
Farris Engineering, Room 209
Albuquerque, NM 87131

Jon C. Helton
Dept. of Mathematics
Arizona State University
Tempa, AZ 85287

Dr. P. M. Herttrich
Gesellschaft für Anlagen und
Reaktorsicherheit (GRS) mbH
Schwertnergasse 1
5000 Köln 1
GERMANY

Dr. D.J. Higson
Radiological Safety Bureau
Australian Nuclear Science &
  Technology Organisation
P.O. Box 153
Roseberry, NSW 2018
AUSTRALIA

Dr. Mitsumasa Hirano
Deputy General Manager
Institute of Nuclear Safety
NUPEC
3-6-2, Toranomon, Minato-ku
Tokyo 108
JAPAN

Dr. S. Hirschberg
Paul Scherrer Institute
Vurenlingen and Villigen
CH-5232 Villigen PSI
SWITZERLAND

Steven Hodge
Oak Ridge National Laboratories
P. O. Box Y
Oak Ridge, TN 37831

Gary Holahan
USNRC-AEOD/OSP
MS: T-4A9

N.J. Holloway
A72.1
Atomic Weapons Establishment
Ademaston
Reading RG7 4PR
UNITED KINGDOM

Griff Holmes
Westinghouse Electric Co.
Energy Center East
Bldg. 371
P.O. Box 355
Pittsburgh, PA 15230

William Hopkins
Bechtel Power Corporation
15740 Shady Grove Road
Gaithersburg, MD 20877

Dean Houston
USNRC-ACRS
MS: P-315

Der-Yu Hsia
Institute of Nuclear Energy Research
Lung-Tan 325
TAIWAN

Alejandro Huerta-Bahena
National Commission on Nuclear
  Safety and Safeguards (CNSNS)
Insurgentes Sur N. 1776
C. P. 04230 Mexico, D. F.
MEXICO

Peter Humphreys
US Atomic Energy Authority
Wigshaw Lane, Culcheth
Warrington, Cheshire
UNITED KINGDOM, WA3 4NE

W. Huntington
Commonwealth Edison Co.
LaSalle County Station
RR1, Box 220
2601 North 21st Rd.
Marsielles, IL 61341

J.S. Hyslop
USNRC-RES/PRAB
MS: T-9F31

Idaho National Engineering Lab. (2)
Attn: Doug Brownson
      Darrel Knudson
EG&G MS: 3840
P.O. Box 1625
Idaho Falls, ID 83415

Idaho National Engineering Lab. (2)
Attn: Art Rood
      Mike Abbott
EG&G MS: 2110
P.O. Box 1625
Idaho Falls, ID 83415

Hanspeter Isaak
Abteilung Strahlenschutz
Hauptabteilung für die Sicherheit
  der Kernanlagen (HSK)
CH-5303 Wurenlingen
SWITZERLAND

Brian Ives
UNC Nuclear Industries
P. O. Box 490
Richland, WA 99352

Kamiar Jamili
DP-62/FTN
Department of Energy
Washington, D.C. 20585

Robert Jones
USNRC-NRR/DSSA
MS: O-8E1

Edward Jordan
USNRC-AEOD/DO
MS: T-4D18

Dr. H. Kalfsbeek
DG/XII/D/1
Commission of the European
Communities
Rue de la Loi, 200
B-1049 Brussels
BELGIUM

Yoshio Kano
General Mngr. & Sr. Engineer
Systems Analysis Section
O-arai Engineer. Centr, PNC
Higashi-Ibaraki-gun
Ibaraki-Ken, 133-13
JAPAN

William Kastenberg
UCLA
Boelter Hall, Room 5532
Los Angeles, CA 90024

Barry Kaufer
OECD/NEA
"Le Seine St. Germain" 12
  Boulevard des Iles
92130 Issy-les-Moulineaux
FRANCE

Paul Kayser
Division de la Radioprotection
Avenue des Archiducs, 1
L-1135 Luxembourg-Belair
LUXEMBOURG

Ken Keith
TVA
W 20 D 201
400 West Surmnit Hill
Knoxville, TN 37092

G. Neale Kelly
Commission of the European
  Communities
Joint Research Centre
Rue de la Loi 200
B-1049 Brussels
BELGIUM

John Kelly
Sandia National Laboratories
P. O. Box 5800
MS 0742
Albuquerque, NM 87185

Knolls Atomic Power Laboratory (2)
Attn: Ken McDonough
      Dominic Sciaudone
Box 1072
Schenectady, NY 12301

Dr. K. Koberlein
Gesellschaft für
  Reaktorsicherheit mbH
Forschungsgelände
D-8046 Garching
GERMANY

Alan Kolaczkowski
Science Applications International
  Corporation
2109 Air Park Rd. S. E.
Albuquerque, NM 87106

Jim Kolanowski
Commonwealth Edison Co.
35 1st National West
Chicago, IL 60690

John G. Kollas
Institute of Nuclear Technology and
 Radiation Protection
N.R.C.P.S. "Demokritos"
P.O. Box 60228
GR-153 10 Aghia Paraskevi
Attiki
GREECE

S. Kondo
Department of Nuclear Engineering
Facility of Engineering
University of Tokyo
3-1, Hongo 7, Bunkyo-ku
Tokyo
JAPAN

D. Lamy
CEN/SCK
Dept. Scientific Irradiation
  Experiment & Study BR2
Boeretang, 200
B-2400 Mol
BELGIUM

Dr. J.M. Lanore
CEA/IPSN/DAS
Centre d'Etudes Nucléaires de
  Fontenay-aux-Roses
B.P. n° 6
92265 Fontenay-aux-Roses CEDEX
FRANCE

Jose A. Lantaron
Consejo de Seguridad Nuclear
Sub. Analisis y Evaluaciones
Calle Justo Dorado, 11
28040 Madrid
SPAIN

Josette Larchier-Boulanger
Electricte de France
Direction des Etudes Et Recherches
30, Rue de Conde
75006 Paris
FRANCE

H. Larsen
Head of Department
Riso National Laboratory
P.O. Box 49
DK-4000 Roskilde
DENMARK

Lawrence Livermore Nat'l Lab. (4)
Attn: George Greenly
      Marvin Dickerson
      Rolf Lange
      Sandra Brereton
Livermore, CA 94550

Shengdar Lee
Yankee Atomic Electric Company
580 Main St.
Boston, MA 17407

B.T.F. Liwaang
Dept. of Plant Safety Assessment
Swedish Nuclear Power Inspec.
P.O. Box 27106
S-10252 Stockholm
SWEDEN

Peter Lohnberg
Expresswork International, Inc.
1740 Technology Drive
San Jose, CA 95110

Steven M. Long
USNRC-NRR/SPSB
MS: O-10E4

D. Eugenio Gil Lopez
Consejo de Seguridad Nuclear
Calle Justo Dorado, 11
28040 Madrid
SPAIN

Los Alamos National Laboratory (2)
Attn: Kent Sasser
N-6, K-557
Los Alamos, NM 87545

Christiana H. Lui
USNRC-RES/PRAB
MS: T-9F31

John Luke
Florida Power & Light
P.O. Box 14000
Juno Beach, FL 33408

Daniel Manesse
ISPN
Boite Postale n° 6
92265 Fontenay-aux-Roses CEDEX
FRANCE

Fred Mann
Westinghouse Hanford Co.
WIA-53
P.O. Box 1970
Richland, WA 99352

Nadia Soido Falcao Martins
Comissao Nacional de Energia Nuclear
R General Severianao 90 S/408-1
Rio de Janeiro
BRAZIL

Harry F. Martz
Analysis and Assessment Division
Los Alamos National Laboratory
Los Alamos, NM 87545

Herbert Massin
Commonwealth Edison Co.
35 1st National West
Chicago, IL 60690

Hideo Matsuzuru
Tokai Research Establishment
Tokai-mur
Maka-gun
Ibaraki-ken, 319-11
JAPAN

Jim Mayberry
Ebasco Services
60 Chubb Ave.
Lyndhurst, NJ 07071

Andrew S. McClymont
IT-Delian Corporation
1340 Saratoga-Sunnyvale Rd.
Suite 206
San Jose, CA 95129

Michael McKay
Los Alamos National Laboratory
A-1, MS F600 Services
P.O. Box 1663
Los Alamos, NM87545

Zen Mendoza
SAIC
5150 El Camino Real
Suite C3 1
Los Altos, CA 94022

Dr. J. Mertens
Division of Risk Analysis &
   Reactor Technology
Institute of Safety Research
Research Centre Julich (KFA)
D-52425 Julich
GERMANY

Jim Meyer
Scientech
11821 Parklawn Dr.
Suite 100
Rockville, MD 20852

Joe Minarick
Science Applications Int'l Corp.
301 Laboratory Road
P.O. Box 2501
Oak Ridge, TN 37830

Jose I. Calvo Molins, Head
Division of P.S.A. and Human Factors
Consejo de Seguridad Nuclear
Calle Justo Dorado, 11
28040 Madrid
SPAIN

Ken Muramatsu
Risk Analysis Laboratory
Japan Atomic Energy Research
Institute
Tokai-mura, Naka-gun
Ibaraki-ken, 319-11, Tokyo
JAPAN

Joseph A. Murphy
Division of Safety Issue Resolution
U.S. Nuclear Regulatory Commission
MS: T-10E50
Washington, DC 20555

Kenneth G. Murphy, Jr.
US Department of Energy
19901 Germantown Rd.
Germantown, MD 20545

Shankaran Nair
Central Electricity
   Generating Board
Berkeley Nuclear Laboratories
Berkeley
Gloucestrshire CL13 9PB
UNITED KINGDOM

Ray Ng
NEI
1776 Eye St. N
Suite 300
Washington, DC 20006-2496

G. Niederauer
Los Alamos National Laboratory
P. O. Box 1663
MSK 575
Los Alamos, NM 87545

Oak Ridge National Laboratory (2)
Attn: Steve Fisher
      Sherrel Greene
MS-8057
P.O. Box 2009
Oak Ridge, TN 37831

Ken O'Brien
University of Wisconsin
Nuclear Engineering Dept.
153 Engineering Research Blvd.
Madison, WI 53706

Theresa Oh
INEL Tech Library
EG&G MS: 2300
P. O. Box 1625
Idaho Falls, ID 83415-2300

N. R. Ortiz, Director
Nuclear Energy Technology
Division 6400
Sandia National Laboratories
Albuquerque, NM 87185

Robert Ostmeyer
U.S. Department of Energy
Rocky Flats Area Office
P. O. Box 928
Golden, CO 80402

Robert Palla
USNRC-NRR/SPSB
MS: O-10E4

Gareth Parry
NUS Corporation
910 Clopper Rd.
Gaithersburg, MD 20878

Vern Peterson
Building T886B
EG&G Rocky Flats
P.O. Box 464
Golden, CO 80402

G. Petrangeli
ENEA Nuclear Energy ALT Disp
Via V. Brancati, 48
00144 Rome
ITALY

Ing. Jose Antonio Becerra Perez
Comision Nacional De Seguridad
   Nuclear Y Salvaguardias
Insurgentes Sur 1806
01030 Mexico, D. F.
MEXICO

William T. Pratt
Brookhaven National Laboratory
Building 130
Upton, NY 11973

Urho Pulkkinen
Technical Research Centre of
  Finland
Laboratory of Electrical &
  Automation Engineeering
Otakaari 7B, 02150 Espoo 15
FINLAND

Blake Putney
Science Applications
  International Corporation
5150 El Camino Real, Suite C31
Los Altos, Ca 94022

Dr. V. M. Raina
Project Manager-Risk Assessment
Ontario Hydro H11 G1
700 University Ave.
Toronto, Ontario M5G 1X6
CANADA

William Raisin
NEI
1726 M. St. NW
Suite 904
Washington, DC   20036

Ann Ramey-Smith
USNRC-RES/PRAB
MS: T-9F31

Dale Rasmuson
USNRC-AEOD/TPAB
MS: T-4A9

John Ridgely
USNRC-RES/SAIB
MS: T-10F13

Richard Robinson (2)
USNRC-RES/PRAB
MS: T-9F31

M. Roch
Manager of Design, Nuclear
  Department
TRACTEBEL
Avenue Ariane 7
B-1200 Bruxelles
BELGIUM

A.E. Rogers
General Electric Co
175 Curtner Ave
MC-489
San Jose, CA 95125

Judy Rollstin
GRAM Inc
8500 Menual Blvd. NE
Albuquerque, NM 87112

Marc Rothschild
Halliburton NUS
1303 S. Central Ave.
Suite 202
Kent, WA 98032

Christopher Ryder
USNRC-RES/PRAB
MS: T-9F31

Takashi Sato, Deputy Manager
Nuclear Safety Engineering Section
Reactor Design Engineering Dept.
Nuclear Energy Group, Toshiba Corp.
Isogo Engineering Center
8, Shinsugita-cho, Isogo-ku,
Yokohama 235, JAPAN

Martin Sattison
Idaho National Engineering Lab.
P. O. Box 1625
Idaho Falls, ID   83415

Dr. U. Schmocker
Hauptabteilung für die
  Sicherheit der Kernanlagen
CH-5232 Villigen HSK
SWITZERLAND

A.J. Seebregts
ECN Nuclear Energy
Westerduinweg, 3
Postbus 1
NL-1755 Petten ZG
THE NETHERLANDS

Dr. S. Serra
Ente Naxionale per I'Energia
Electtrica (ENEL)
via G.B. Martini 3
I-00198 Rome
ITALY

H. Shapiro
Licensing & Risk Branch
Atomic Energy of Canada Ltd.
Sheridan Park Research Comm.
Mississauga, Ontario L5K 1B2
CANADA

Nathan O. Siu
Center for Reliability and Risk
  Assessment
Idaho National Engineering Lab.
EG&G MS: 3850
P.O. Box 1625
Idaho Falls, ID 83415-3855

E. Soederman
ES-Konsult AB
Energy and Safety
P.O. Box 3096
S-16103 Bromma
SWEDEN

Desmond Stack
Los Alamos National Laboratory
Group Q-6, Mail Stop K556
Los Alamos, NM 87545

Jao Van de Steen
KEMA Laboratories
Utrechtseweg, 310
Postbus 9035
NL 800 ET Arnhem
THE NETHERLANDS

Eli Stern
Israel AEC Licensing Div.
P.O. Box 7061
Tel-Aviv 61070
ISRAEL

Dr. Egil Stokke
Advisory Group
OECD Halden Reactor Project
P.O. Box 173
N-1751 Halden
NORWAY

Stone & Webster Engineering Corp
Technical Information Center
A. Hosford
245 Summer Street
245/01
Boston, MA 02210

Dennis Strenge
Pacific Northwest Laboratory
RTO/ 125
P.O. Box 999
Richland, WA 99352

Technadyne Engineer. Consultants (3)
Attn: David Chanin
      Jeffery Foster
      Walt Murfin
Suite A225
8500 Menual Blvd. N
Albuquerque, NM 87112

Ashok Thadani
USNRC-NRR/ADT
MS: O-12G18

T. G. Theofanous
University of California, S. B.
Department of Chemical and Nuclear
  Engineering
Santa Barbara, CA 93106

Catherine Thompson
USNRC-RES/SAIB
MS: T-10F13

Soren Thykier-Nielsen
Riso National Laboratory
Postbox 49
DK4000 Roskile
DENMARK

R. Toossi
Physical Research, Inc.
25500 Hawthorn Blvd.
Torrance, CA 90505

Ennio Traine
ENEL
Via Vialiano, 48
00144 Rome
ITALY

Ulf Tveten
Environmental Physics Section
Institutt for Energiteknikk
Postboks 40
N-2007 Kjeller
NORWAY

US Department of Energy
Energy Library
Room G 034/GTN
AD-622.1
Washington, DC 20585

US Department of Energy
NS-50 (GTN)
NS-10.1
S-161
Washington, DC 20585

U.S. Environmental
    Protection Agency (2)
Attn: Allen Richardson
      Joe Logsdon
Office of Radiation Programs
Environmental Analysis Division
Washington, DC 20460

Harold VanderMolen
USNRC-RES/PRAB
MS: T-9F31

Dr. A. Valeri
A.N.P.A.
Via Vitaliano Brancati, 48
I-00144 Rome
ITALY

Magiel F. Versteeg
Ministry of Social Affairs
    and Employment
P.O. Box 90804
2509 LV Den Haag
THE NETHERLANDS

Martin Virgilio
USNRC-NRR/DSSA
MS: O-8E2

R. Virolainen, (Chairman PWG5)
Systems Integ. Off. (STUK)
P.O. Box 268
Kumpulanite 7
SF-60101 Helsinki
FINLAND

Seppo Vuori
Technical Research Centre of Finland
Nuclear Engineering Laboratory
Lonnrotinkatu 37
P.O. Box 169
Sf-00181 Helsinki 18
FINLAND

Dr. Ian B. Wall
81 Irving Avenue
Atherton, CA 94027

Edward Warman
Stone & Webster Engineering Corp.
P.O. Box 2325
Boston, MA 02107

J.E. Werner
Reactor Research & Techn Division
US DOE Idaho Operations
MS: 1219
850 Energy Drive
Idaho Falls, ID 83401-1563

Dr. Wolfgang Werner
Safety Assessment Consulting GmbH
Veilchenweg 8
D 83254 Breitbrunn
GERMANY

Westinghouse Electric Corp
Technical Library
P. O. Box 355
East 209
Pittsburgh, PA 15230

Westinghouse Electric Corp
NTD
Central File Nuclear Safety
P. O. Box 355
408 1-A
Pittsburgh, PA 15230

Westinghouse Electric Company (3)
Attn: John Lacovin
      Burt Morris
      Griff Holmes
Energy Center East, Bldg. 371
P.O. Box 355
Pittsburgh, PA 15230

Westinghouse Savannah River Co. (2)
Attn: Kevin O'Kula
       Jackie East
Safety Technology Section
1991 S. Centennial Ave., Bldg. 1
Aiken, SC 29803

Donnie Whitehead
Department 6412, MS: 0747
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0747

Keith Woodard
PLG, Inc.
7315 Wisconsin Ave.
Suite 620 East
Bethesda, MD 20814-3209

John Wreathall
John Wreathall & Co.
4157 MacDuff Way
Dubin, OH 43017

M. K. Yeung
University of Hong Kong
Mechanical Engineering Dept.
Polfulam
HONG KONG

Bob Youngblood
Brookhaven National Laboratory
Department of Nuclear Energy
Bldg. 130
Upton, NY 11973

Carlo Zaffiro
A.N.P.A.
Directorate for Nuclear
Via Vitaliano Brancate, 48
I-00144 Rome
ITALY

Dr. X. Zikidis
Greek Atomic Energy Comm.
N.R.C.P.S. "Demokritos"
GR-153 10 Agia Paraskevi
Attiki
GREECE

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-6093 BNL-NUREG-52388 SAND93-1804

2. TITLE AND SUBTITLE

An Analysis of Operational Experience During Low Power and Shutdown and a Plan for Addressing Human Reliability Assessment Issues

3. DATE REPORT PUBLISHED

MONTH	YEAR
June	1994

4. FIN OR GRANT NUMBER
L2415, L2539

5. AUTHOR(S)
M. Barriere, W. Luckas/BNL, D. Whitehead/SNL, A. Ramey-Smith/NRC

6. TYPE OF REPORT

Technical

7. PERIOD COVERED *(Inclusive Dates)*

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

Brookhaven National Laboratory
Upton, NY 11973

Sandia National Laboratories
Albuquerque, NM 87185

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

10. SUPPLEMENTARY NOTES

11. ABSTRACT *(200 words or less)*

Recent nuclear power plant events (e.g. Chernobyl, Diablo Canyon, and Vogtle) and U.S. Nuclear Regulatory Commission (NRC) reports (e.g. NUREG-1449) have led to concerns regarding human reliability during low power and shutdown (LP&S) conditions and limitations of human reliability analysis (HRA) methodologies in adequately representing the LP&S environment. As a result of these concerns, the NRC initiated two parallel research projects to assess the influence of LP&S conditions on human reliability through an analysis of operational experience at pressurized water reactors (PWRs) and boiling water reactors (BWRs). These research projects, performed by Brookhaven National Laboratory for PWRs, and Sandia National Laboratories for BWRs, identified unique aspects of human performance during LP&S conditions and provided a program plan for research and development necessary to improve existing HRA methodologies. This report documents the results of the analysis of LP&S operating experience and describes the improved HRA program plan.

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

human reliability analysis (HRA), low power and shutdown (LP&S), PRA

13. AVAILABILITY STATEMENT

Unlimited

14. SECURITY CLASSIFICATION

(This Page)
Unclassified

(This Report)
Unclassified

15. NUMBER OF PAGES

16. PRICE

NRC FORM 335 (2-89)