Enclosure 4

MFN 07-063

ESBWR Human Factors Engineering

Licensing Topical Report NEDO-33262

ESBWR HFE Operating Experience Review Implementation Plan Revision 1

GE Energy
Nuclear

3901 Castle Hayne Rd
Wilmington, NC 28401

NEDO 33262
Revision 1
Class I
DRF#0000-0049-8918
January 2007

LICENSING TOPICAL REPORT

ESBWR HFE OPERATING EXPERIENCE REVIEW IMPLEMENTATION PLAN

INFORMATION NOTICE

This document, NEDE-33262 Revision 1, contains no proprietary information.

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT PLEASE READ CAREFULLY

The information contained in this document is furnished for the purpose of obtaining NRC approval of the ESBWR Certification and implementation. The only undertakings of General Electric Company with respect to information in this document are contained in contracts between General Electric Company and participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone other than that for which it is intended is not authorized; and with respect to **any unauthorized use**, General Electric Company makes no representation or warranty, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document.

Table of Contents

1 OVERVIEW

As part of the Human Factor Engineering process shown in Figure 1 operating experience reviews (OERs) are conducted to identify HFE-related safety and availability issues. The OER obtains and analyzes information on the past performance of predecessor designs. In the case of a new plant such as the ESBWR, the evolution of the design comes from years of BWR experience and improvements. The ESBWR builds upon the operational experience of the ABWR and the testing and design experience of the SBWR. The issues and lessons learned from previous operating experience provide a basis for improving the plant design and the Human System Interface (HSI) in a timely way; i.e., at the beginning of the design process.

History has demonstrated that valuable lessons can be learned from incidents and accidents. This was demonstrated after the accident at Three Mile Island nuclear power plant in the United States of America in 1979, when far-reaching follow-up actions were taken to minimize the risk of a recurrence and to improve the HSI and procedures for accident management. The accident at Chernobyl demonstrated that the lessons from the Three Mile Island accident had not been acted upon in the USSR: in particular, the importance of systematic evaluation of operating experience, the need to strengthen the on-site technical and management capability, including improved operator training, and the importance of the man-machine interface (IAEA, INSAG-7, 1992).

The analysis of operating experience events to understand the role of human actions provides support during the design for engineering decisions regarding the HSI to enhance safety. The documentation provides a basis for design decisions, and a starting point for developing some performance indicators, an experience review system for the operating plant.

1.1 Purpose

The purpose of this implementation plan is to establish methods, criteria and guidance for identifying, analyzing and documenting lessons learned from published reviews of past events, PRA's and other available information sources. The lessons learned and insights gained are used to recommend potential tools and technological solutions to reduce human errors and their impact on risk and reliability of plant operation. In this way, negative features associated with predecessor designs may be avoided in the current design while retaining positive features. This plan document describes a methodology for handling experience information to be performed by the Design Team and the Control Room Design Team (CRDT), as specified in the MMIS and HFE Implementation Plan [2.1.1 (1)].

1.2 Scope

This plan establishes an OER process in conformance with the ESBWR MMIS and HFE Implementation Plan [2.1.1 (1)], and NUREG-0711 Rev. 2, Human Factors Engineering Program Review Model [2.3(4)]. The interaction of the OER subtasks with other HFE tasks is shown in Figures 1, 2, and 3.

Review of experience and identification of problems in prior HSI implementations, including human factors problems, will be addressed throughout the design process. In addition, the ESWBR DCD requires that a review of the industry experience with the operation of those selected HSI equipment technologies be conducted for those designs, which are similar to the proposed design. The review of those HSI technologies includes both a review of literature pertaining to the human factors issues related to similar system applications of those technologies and interviews with personnel experienced with the operation of those systems.

Any relevant HFE issues/concerns associated with the selected HSI equipment technologies are entered into the HFE Issue Tracking System (HFEITS). OER for the ABWR was performed for First-of-a-Kind-Engineering (FOAKE) Operational Experience / Lessons Learned Evaluation (24516-1A10-6110-0001 Rev. 1 (09/23/96). The FOAKE OER results were incorporated into the plant-level design and system-level designs of one ABWR currently under construction. The ESBWR design reflects predecessor BWR and ABWR OER because the ESBWR design incorporates many BWR and ABWR design features. The FOAKE OER will be reviewed to identify predecessor BWR and ABWR operating experience incorporated in the ESBWR design, and operating experience requiring additional review.

The ESBWR HFE team will use OER information, particularly safety lessons learned, for the process of allocating functions to manual, shared, or automated. Lessons learned from a review of previous nuclear plant HSI designs, are entered into the HFEITS to assure that problems observed in previous designs are adequately addressed in the ESBWR design implementation. Also, recognized industry HFE issues such as those documented in NRC documents such as NUREG-0933 and NUREG/CR-6400 are addressed.

A Baseline Review Record (BRR) database, in conjunction with an OER database, will be used by the ESBWR system designers, to analyze risk important HAs. The BRR/OER database provides both predecessor design and operational experience documentation to the ESBWR design team for HFE design evaluation into the ESBWR design. The BRR database establishes guidance for identifying significant differences between the ESBWR design and predecessor designs, as well as establishing a process for evaluation and resolution of identified differences.

The scope of this plan includes the following:

- Establishing a framework and classification system for analyzing the human factor aspects of operating experience. This includes evaluating defenses against potential or actual human errors identified during the HSI design process, and developing criteria for reporting to the operating experience and lessons learned tracking (refer to section 5.2).
- Identifying and reviewing published research documents that address experience with the HSI in different modes of operation and transitions between modes using selected technological approaches (e.g., if touch-screen interfaces are planned, the HFE issues associated with using them should be reviewed).

- Analyzing experience summary documents in detail and integrating the insights that support enhancement of human actions affecting the risk and reliability of both normal and outage operations (e.g., generic safety issues defined by the NRC).
- Classifying and evaluating events reported by BWR and ABWR predecessor systems upon which the design is based, and other plants with similar design features.
- Obtaining and incorporating feedback from utility operators on needs of operators, maintainers, testers, and outage planners.
- Providing input to the HFE Issue Tracking System (HFEITS).

1.3 Definitions and Acronyms

Several terms are defined to provide a common basis for evaluating events and operating experience referred to in the subsequent paragraphs.

1.3.1 Definitions

Accident class: a grouping of severe accidents with similar characteristics (such as accidents initiated by a transient with a loss of decay heat removal, loss of coolant Accidents, station blackout accidents, and containment bypass accidents) (ASME PRA Std.).

Accident situation: An abnormal plant state occurring during an accident, which may lead to a new damage condition. Operating crews' actions can prevent, mitigate or exacerbate the accident progression.

Action task: The "doing" portion of a task, performed by the control room operators or the plant technicians. This involves the physical action of operating control room switches by the control room operators or manipulating or repairing equipment in the plant by the technicians.

At power: those plant operating states characterized by the reactor being critical and producing power, with automatic actuation of critical safety systems not blocked and with essential support systems aligned in their normal power operation configuration.

Cognitive process: An internal, human activity that receives, manipulates, and stores knowledge or information, or which controls actions according to this knowledge.

Cognitive task: The thinking portion of a task, often performed by the control room operators. This involves determining the present condition or state of the plant and the proper recovery action(s) to be performed.

Consequences: The results of (i.e., events that follow and depend upon) a specified event.

Contingencies: Pre-thought out plans for mitigating undesired events that occur during plant operations.

Control Function: "Keeping measured functional parameters within bounds though a process of manipulating low level functions to satisfy a higher level function" (NUREG-0711, Rev. 2, page 96, [2.3(4)]).

Control Room Design Team (CRDT): is a subset of the Design Team. The CRDT is responsible for the overall coordination of the design of the Main Control Room (MCR), Remote Shutdown System (RSD) Panels, and applicable Local Control Stations.

Crew: The group of people at the plant that manage and perform activities that are modeled in the PRA.

Diagnosis: examination and evaluation of data to determine either the condition of a SSC or the cause of the condition (ASME PRA Std).

Failure mechanism: any of the processes that results in failure modes, including chemical, electrical, mechanical, physical, thermal, and human error (ASME PRA Std).

Failure mode: a condition or degradation mechanism that precludes the successful operation of a piece of equipment, a component, or a system (ASME PRA Std).

Framework: A systematic organization of tasks or activities used in a specified type of analysis.

Front-line system: an engineered safety system used to provide core or containment cooling, reactivity control or pressure control, and to prevent core damage, reactor coolant system failure, or containment failure (ASME PRA Std).

Function: An activity or role performed by a human, structure, or automated system to fulfill an objective (System Functional Requirements Analysis Implementation Plan [2.1(3)]).

Human error: Can be defined as a mismatch between a performance demand and the human capability to satisfy that demand.

Human error recovery: The human ability to recognize and correct an error before the error becomes irreversible.

Human interaction: A human action or set of actions that affects equipment or physical systems, or an action that influences other human actions. Human interactions can be represented as an event in a fault tree or branch point in an event tree.

Human reliability analysis (HRA): a structured approach used to identify potential human failure events and to systematically estimate the probability of those errors using data, models, or expert judgment (ASME PRA Std).

Human Task: The activity of a human required to accomplish a function. For example the human user conserves, reduces, or adds information, and supplies or controls energy.

Human-induced initiators: Errors in human activities conducted during normal operation that cause an off normal condition and are typically included as contributors to initiating events or revealed system faults (i. e., Type B human errors).

Human-System Interface (HSI): The organization of inputs and outputs used by personnel to interact with the plant, including the alarms, displays, controls, and job performance aids. Generically, this includes maintenance, test, and inspection interfaces as well.

Initiating event: any event either internal or external to the plant that perturbs the steady state operation of the plant, if operating, thereby initiating an abnormal event such as transient or LOCA within the plant. Initiating events trigger sequences of events that challenge plant control and safety systems whose failure could potentially lead to core damage or large early release.

Intervention: Countermeasures that can be taken (during the design) to either prevent errors from occurring in the first place or correct them once they do occur. Interventions can include tools, computers, software, training, procedures and documentation, guidelines, work practices, man-machine interface, job performance aids, support systems, and work planning aids.

Less than full power: All operating states other than full power.

Local Control Station (LCS): An operator interface related to nuclear power plant (NPP) process control that is not located in the main control room. This includes multifunction panels, as well as single-function LCSs such as controls (e.g., valves, switches, and breakers) and displays (e.g., meters) that are operated or consulted during normal, abnormal, or emergency operations.

Machine Task: The activity of a machine in accomplishing a function by supplying whatever information or energy is required. The machine includes both hardware and software.

Maintenance: Activities carried out to keep systems and equipment available. Specific types of maintenance include preventive, and corrective. Activities associated with preventive maintenance include testing, surveillance, inspection, and calibration. Activities associated with corrective maintenance include repair, replace, and modify.

Mistake: A category of human errors where a wrong action was taken or the correct action was not taken because the intent for the action was formed incorrectly.

MMIS Design Team: The MMIS Design Team (Design Team) is a team of engineers, as defined in the MMIS and HFE Implementation Plan, responsible for the design of the MMIS systems.

Operating time: total time during which components or systems are performing their designed function (ASME PRA Std).

Operating experience review: A systematic review, analysis and evaluation of operating experience that can apply to the development of the man machine interface design.

Performance shaping factor (PSF): a factor that influences human error probabilities as considered in a PRA's human reliability analysis and includes such items as level of training, quality/availability of procedural guidance, time available to perform an action, etc. (ASME PRA Std).

Performance shaping factors: Physiological, psychological, and environmental influences affecting human performance.

Plant-specific data: data consisting of observed sample data from the plant being analyzed (ASME PRA Std).

Post-initiator actions: After a transient has been initiated, human actions are often required to return the plant to normal operation or achieve a safe plant shutdown. These actions are typically described in procedures. Errors in the procedural response actions or additional component failures, lead to new situations where operators must recover inoperable equipment or find alternative methods for controlling the event. Such recovery actions are not specifically described in procedures, but rely on the training knowledge of the crew. Human actions that required a defined response and/or equipment restoration can be defined in the PRA from review of the cutsets, accident sequences or grouped scenarios (i.e., Type C human errors).

Post-initiator human failure events: human failure events that represent the impact of human errors committed during actions performed in response to an accident initiator (ASME PRA Std).

Pre-initiator events: Errors in human activities such as maintenance, testing and calibration conducted during normal operation can lead to inoperable equipment without causing a transient. The important errors are those that defeat redundant or diverse systems required for safety and leave the system in an unrevealed fault state (i. e., Type A latent human errors).

Pre-initiator human failure events: human failure events that represent the impact of human errors committed during actions performed prior to the initiation of an accident, (e.g., during maintenance or the use of calibration procedures) (ASME PRA Std).

Recovery: a general term describing restoration and repair acts required to change the initial or current state of a system or component into a position or condition needed to accomplish a desired function for a given plant state (ASME PRA Std).

Recovery action: a human action performed to regain equipment or system operability from a specific failure or human error in order to mitigate or reduce the consequences of the failure (ASME PRA Std).

Recovery: (1) A set of interactions intended to restore failed equipment or to find alternatives to achieve their function, or (2) the event that represents (1).

Response: – to react to a cue for action in initiating or recovering a desired function.

Revealed Fault: A system or plant fault that is immediately detectable by observation or instruments. They stem from either hardware faults or human induced initiators (Type B human errors).

Safety systems: those systems that are designed to prevent or mitigate a design-basis accident (ASME PRA Std).

Screening analysis: an analysis that eliminates items from further consideration based on their negligible contribution to the probability of a significant accident or its consequences (ASME PRA Std).

Screening criteria: the values and conditions used to determine whether an item is a negligible contributor to the probability of an accident sequence or its consequences (ASME PRA Std).

Severe accident: an accident that involves extensive core damage and fission product release into the reactor vessel and containment, with potential release to the environment (ASME PRA Std).

Slip: A category of human errors where the intent to take the correct action was formed, but because of the physical or mental environment a wrong action was taken or the correct action was not taken.

Success criteria: criteria for establishing the minimum number or combinations of systems or components required to operate, or minimum levels of performance per component during a specific period of time, to ensure that the safety functions are satisfied. (ASME PRA Std.)

Support system: a system that provides a support function (e.g., electric power, control power, or cooling) for one or more other systems (ASME PRA Std).

System failure: termination of the ability of a system to perform any one of its critical design functions. Note: Failure of a line/train within a system may occur in such a way that the system retains its ability to perform all its required functions; in this case, the system has not failed. (ASME PRA Std)

Task: A collection of activities with an identifiable start and end point for which human actions are performed.

Unavailability: the fraction of time that a system or component is not capable of supporting its function including but not limited to the time it is disabled for test or maintenance (ASME PRA Std).

Unrevealed fault: A system or plant fault undetected by observation or instruments. They stem from either undetected hardware faults or pre-initiator human errors (Type A human errors).

1.3.2 Acronyms

The following is a list of acronyms used in this plan:

ASME	American Society of Mechanical Engineers
BRR	Baseline Review Record
CRDT	Control Room Design Team
CRT	Cathode Ray Tube
FRA	Functional Requirement Analysis
HED	Human Error Discrepancy
HRA	Human Reliability Analysis
HFE	Human Factor Engineering
HFEITS	Human Factor Engineering Issue Tracking System
HSI	Human System Interface
LCS	Local Control Station
LOCA	Loss of Coolant Accident
MCR	Main Control Room
MMIS	Man-Machine Interface Systems
NPP	Nuclear Power Plant
OER	Operating Experience Review
PRA	Probability Risk Assessment
PSF	Performance Shaping Factor
SDC	Shut Down Cooling
SRO	Senior Reactor Operator
SSC	Systems, Structures, and Components
Std	Standard
TA	Task Analysis
VDU	Video Display Unit

2 APPLICABLE DOCUMENTS

Applicable documents include supporting documents, supplemental documents, codes and standards and are given in this section. Supporting documents provide the input requirements to this plan. Supplemental documents are used in conjunction with this plan. Codes and standards are applicable to this plan to the extent specified herein.

2.1 Supporting and Supplemental Documents

2.1.1 Supporting Documents

The following supporting documents were used as the controlling documents in the production of this plan. These documents form the design basis traceability for the requirements outlined in this plan.

1. NEDO-33217, Rev 2, ESBWR Man-Machine Interface Systems and Human Factors Engineering Implementation Plan
2. ESBWR Design Control Document, Chapter 18, Rev. 3 (GE 26A6642BX)
3. NEDO-33181, Rev 0, NP-2010 COL Demonstration Project Quality Assurance Plan

2.1.2 Supplemental Documents

The following supplemental documents are used in conjunction with this document plan.

1. First-of-a-Kind Engineering Program (FOAKE) Operational Experience/Lessons Learned Evaluation, (24156-1A10-6110-0001) Rev. 1 (09/23/96)
2. GE Advanced Boiling Water Reactor Standard Safety Analysis Report (SSAR), Rev 8, 23A6100
3. NEDO-33219, Rev 1, ESBWR System Functional Requirements Analysis Implementation Plan
4. NEDO-33221, Rev 1, ESBWR Task Analysis Implementation Plan
5. NEDO-33267, Rev 1, ESBWR Human Reliability Analysis Implementation Plan
6. NEDO-33276, Rev 1, ESBWR Human Factors Verification and Validation Implementation Plan

2.2 Codes and Standards

The following codes and standards are applicable to the HFE program to the extent specified herein.

1. ASME, Standard for Probabilistic Risk Assessment For Nuclear Power Plant Applications, 2002

2. IEEE 1023, Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations, 2004

3. IEEE 845, Guide to the Evaluation of Human-System Performance in Nuclear Power Generating Stations, 1999

2.3 Regulatory Guidelines

1. NUREG-4674, Precursors to Potential Severe Core Damage Accidents: 1984 to 1989, Status Reports, Volumes 1-11 1986 to 1991

2. NUREG-6400, HFE Insights For Advanced Reactors Based Upon Operating Experience, 1996

3. NUREG-0700, Human System Interface Design Review Guideline, Rev. 2, 2002 (U.S. Nuclear Regulatory Commission).

4. NUREG-0711, Human Factors Engineering Program Review Model, Rev. 2, 2004

5. NUREG-0933, A Prioritization of Generic Safety Issues, 2005

6. NUREG-1269, Loss of Residual Heat Removal System Unit 2, 1987

7. NUREG-1449, Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States Draft for Comment, Sept.1993

2.4 DOD and DOE Documents

1. AD/A223-168, System Engineering Management Guide, 1990

2.5 Industry / Other Documents

Reference documents that have been removed may be re-added to the next revision, as they become available to the HFE design team.

1. Decision Analysis and Behavioral Research, D. Winterfeld and W. Edwards. Cambridge: Cambridge University Press, 1986.

2. IAEA Safety Series No. 75- INSAG-12, Rev. 1, Basic Safety Principles for Nuclear Power Plants, 1999

3. IAEA Safety Series No. 75-INSAG-3: Basic Safety Principles for Nuclear Power Plants, 1988.

4. IAEA Safety Series No. 75- INSAG-7 The Chernobyl Accident: Updating of INSAG-1, 1992

5. IAEA Safety Series No. 75- INSAG-10: Defense-In-Depth in Nuclear Safety, 1996.

6. IEC 964, Design for Control Rooms of Nuclear Power Plants, 1989

7. Information processing and human-machine interaction, an approach to cognitive engineering, J. Rasmussen, 1986

8. Institute of Nuclear Power Operations Performance Indicator Reports 1982 to 1992, 1992

9. NSAC-083, Brunswick Decay Heat Removal Probabilistic Safety Study, 1985

10. NSAC-088, Residual Heat Removal Experience Review and Safety Analysis Boiling Water Reactors, 1986

11. NUMARC 91-06, "Guidelines to Enhance Safety During Shutdown," Dec 1991

3 METHODS

Review of experience and identification of problems in prior HSI implementations, including human factors problems, are addressed throughout the design process. In addition, the ESWBR DCD requires that a review of the industry experience with the operation of those selected HSI equipment technologies will be conducted for those designs, which are similar to the proposed design.

The review of those HSI technologies will include both a review of literature pertaining to the human factors issues related to similar system applications of those technologies and interviews with personnel experienced with the operation of those systems. Any relevant HFE issues/concerns associated with the selected HSI equipment technologies will be entered into the HFE Issue Tracking System (HFEITS).

Lessons learned from a review of previous nuclear plant HSI designs, will be entered into the HFEITS to assure that problems observed in previous designs will be adequately addressed in the ESBWR design implementation. Also, recognized industry HFE issues such as those documented in NUREG/CR-6400 will be addressed.

Personnel interviews will be conducted to determine the operating experience related to predecessor plants or systems. The topics included in the interviews as a minimum will be plant operations and HFE Design topics.

Reviews of operating experience are conducted for the following HSI design areas. The review areas include plant operations and HFE design topics. Plant operations address normal plant evolutions, instrument failures, HSI equipment and process failures, transient, accidents and reactor shutdown periods, and cooldown using a remote shutdown system.

HFE Design Topics include decisions about selection of alarm and annunciation elements, displays, control and automation elements, information processing and job aids, real-time communications with plant personnel and other organizations, procedures, training, staffing/qualifications, and job design. For example, new elements of the HSI design, in which further development of the industry is expected include:

1. Use of flat panel display panels and CRT/VDU displays
2. Use of CRTs in selected applications
3. Use of touch screen technology vs. other types of pointing/input devices
4. Use of electronic on-screen controls
5. Use of wide display panels
6. Use of prioritized alarm systems
7. Automation of process systems
8. Operator workstation design integration

9. Any other areas where clear industry developments have been made which may address HSI and HFE areas

These operating experience reviews include review of:

1. Recognized industry HFE Issues (e.g., NUREG/CR-6400)
2. Reports provided by industry organizations such as EPRI
3. Review of applicable research in these design areas
4. Proceedings published by HFE professional societies
5. Review of applicable research and experience reports published by HSI equipment vendors
6. Review with actual users or industries (e.g., non nuclear power generation, process industries, aerospace, DOD, etc.) of the new elements of HSI design

As developed from Table 3.1 of NUREG 0711, Rev 2, Figure 3 shows a process for the OER contribution to support key HFE task elements addressed in the MMIS and HFE Implementation Plan :

1. Functional Requirements Analysis
2. Function Allocation
3. Task Analysis
4. Human Reliability
5. Plant Staffing/Qualifications
6. Human-System Interface
7. Procedures (operating, maintenance, testing, and surveillance.)
8. Training
9. Human Factors Verification and Validation

3.1 Plant Operations

3.1.1 Background

The following areas have been identified in NUREG-0711 Rev. 2 as potential topics for conduct of interviews with experienced operators. The intent is to receive candid inputs from plant staff that may not be provided in published reports. Design teams from predecessor design also serve as potential contributors for OERs. The information gathered should be based upon facts, such as the results of evaluations or test results, rather than based upon personal opinions.

3.1.2 Goals

The goal of the OER of plant operations is the identification and analysis of HFE related safety issues and problems of the past performance of predecessor designs. For the ESBWR, this includes earlier design for which the new design is based.

3.1.3 Basis and Requirements To Plant Operations Review

The OER of plant operations is reviewed and verified to ensure that the identification and analysis of HFE-related problems and issues, using the criteria in the General Approach section 3.1.4 below, have been met.

The HFE design team interviews plant operations personnel and previous HFE team members and personnel from the ABWR predecessor plant and previous BWR plants. The HFE design team interviews operators who are involved with the full-scale simulator training for additional OER input.

3.1.4 General Approach To Plant Operations Review

As a minimum the following serves as candidate topics for an OER:

1. Plant operations address normal plant evolutions
2. Instrument failures
3. HSI equipment and processor failures
4. Plant transients
5. Accidents and reactor shutdown periods and cool down using a remote shutdown system

3.1.5 Application

3.2 HSI Topics

The OER of HFE Design HSI Topics is identified in NUREG-0711, Rev. 2. The identified HFE Design Topics have been, in the past, areas of HFE related problems and other issues affecting the safe and efficient operations of the plant. The issues and lessons learned from the operating experience on the HFE Design Topics from predecessor designs provide a basis for improving the ESBWR plant design.

3.2.1 Goals

The goals of the OER of HFE Design Topics are to identify and analyze HFE related safety issues and problems with specific design features using past performance of predecessor designs and tests related to the specific design features.

3.2.2 Basis and Requirements To HSI Topics Review

The OER of plant operations is reviewed and verified to ensure that the identification and analysis of HFE-related problems and issues, using the criteria in the general approach section 3.2.3 below, have been met.

3.2.3 General Approach To HSI Topics Review

HFE overall plant design rules for topics and technologies related to HSI will be described in the HFE style guide. The style guide will consider the criteria from NUREG-0711, Rev. 2 as applied to the modern HSI designs. The following recommended topics from NUREG 0711 Rev. 2 are:

1. Alarm and annunciation
2. Display of plant information and controls
3. Control and automation
4. Information processing and job aids
5. Real-time communications with plant personnel and other organizations
6. Procedures, training, staffing/qualifications, and job design

3.2.3.1 Sources of information for ESBWR experience review

The MMIS Design Team ensures that operating experience and the results of research relevant to safety are identified, reviewed, and analyzed, and that the lessons learned are incorporated into the HSI as practical. These operating experience reviews include screening and analysis of:

1. Nuclear Regulatory Reports

- NUREG reports
- AEOD event evaluation reports
- Nuclear Reactor Regulation Reports
- Sponsored Research and National Lab reports (e.g., NUREG/CR-6400)
- Event Reports

2. Nuclear Industry Reports

- EPRI reports
- NUMARC Guidelines
- INPO reports

- NSAC Event Evaluation reports
- Less than full power or shutdown Probabilistic Risk Studies
- Utility personnel interviews

3. Other reports and information

- Review of applicable research in the technologies considered for the design
- Review of proceedings published by HFE professional societies
- Review of R&D and experience reports published by HSI equipment vendors
- Review with actual users in other industries (e.g., non nuclear power generation, process industries, aerospace, DOD, etc.) of the above technologies
- Review of FOAKE Engineering Program, Operational Experience / Lessons Learned Evaluation (24516-1A10-6110-0001), Rev. 1, 09/23/96

3.2.3.2 Review of experience information

Reviews of documents related to the HSI design can range from evaluation of single event reports to consideration of summarized analysis of many related events. If summarized data are already well analyzed by others and applicable to the current ESBWR HSI design, the need to review single event reports by the HFE team is reduced. If there are cases in the HSI designs where experience events are unavailable for evaluating the design, substitute events can be developed through the use of the PRA/HRA internal events study accident scenarios.

The HFE Issue Tracking System, described in [2.1.1 (1)], will assure that HFE issues/concerns of OER that are identified throughout the development and evaluations of the HSI implementation are addressed. The Control Room Design Team (CRDT) will prepare a risk based administrative procedure which define the criteria used to decide what OER issues will go into the HFE Issue Tracking System.

3.2.3.3 Screening

Some reports may be remotely related to the issues of designing the ESBWR HSI and some might be very relevant. There are large numbers of reports on human related events in Nuclear power plants both domestically and international. To make efficient use of time, the documents identified above need to be prioritized and screened for applicability to the design process. This involves several screening steps in addressing to find the best information on safety or availability issues, the relative importance to changes in the design, the mode of operation etc. Once information is in the BRR/OER database, the results can be queried to support other HFE tasks as needed.

3.2.3.4 Classification

The level of classification can be developed from both the task analysis classification issues and HRA information. The task analysis looks at the features required to do a task and the HRA uses models and/or data to quantify the likelihood for human errors.

The individual OER information file(s) will be screened and classified for the human factors aspects of operating experience, according to a scheme and/or framework to be developed, section 1.2. The scheme will reflect the commonality between the combined issues from the various sources. The classification scheme will consider the critical tasks identified in HRA Implementation Plan [2.1.2 (5)], the HRA risk informed decision making identified in the Task Analysis Implementation Plan and other HFE activities. The purpose of the classification is to place issues into categories that can facilitate their disposition. For example there may be a number of specific responses relating to problems and suggestions for improvements assigned to the classification for nuisance alarming during emergency events.

3.2.3.5 Identification of human Issues

Once the event data or analyzed reports are selected and considered for ESBWR design HFE support, they can be analyzed to identify problematic operations and tasks and point to potential human factor enhancements for all aspects of human performance. This includes the Human System Interface design, procedures, personnel training, and control room staffing and qualifications.

The ESBWR design is an extension of the ABWR design that is an extension of the BWR design. Previous OER's were reviewed and actions were taken to minimize or eliminate identified human interaction deficiencies at BWR/ABWR plants. This philosophy will continue with the ESBWR design.

The example in Appendix A, links events that have occurred during shutdown conditions at nuclear power plants involving human interactions. This work was compiled in 1992-1993 from NRC reports, LERs, EPRI reports, PRA models and information from INPO provided by EPRI. The lessons learned and recommendations from this study along with other OER results will be reviewed by the ESBWR HFE design team and applicable items entered into the Human Factors Engineering Issue Tracking System (HFEITS) for resolution. This process will provide input into the ESBWR design, operator training and procedure improvements.

3.2.4 Application

Identify risk-important HAs in the predecessor and similar plant designs to determine if they are risk-important in the design. For those that are applicable, identify those scenarios where these actions were called for during operation of the plant and if the actions were successfully completed, noting aspects of the design that helped to assure success. If errors have occurred in

their execution, insights should be identified related to needed improvements in human performance.

Where the risk-important HAs are determined to be different from those of the predecessor plant, identify any operating experience related to these different risk-important human actions.

Identify those risk-important HAs from the OER requiring special attention during the design process and any insights that would be beneficial during the HFE design and implementation process.

4 IMPLEMENTATION

4.1 Operating Experience Review

4.1.1 Assumptions

The Operating Experience Review of Plant Operations identifies HFE-related safety issues. The lessons learned from operating experience provide a basis for improving the plant design, especially at the beginning of the design process.

4.1.2 Inputs

1. Nuclear Regulatory reports
2. Nuclear Industry Reports
3. HFE Design Team interviews with plant operations personnel.
4. Review of applicable research in the technologies considered for the design.
5. BRR/OER Database

4.1.3 Process

4.1.3.1 Reliability Evaluations

The HSI implementation process establishes reliability and availability criteria for each component part of the HSI within the design and procurement specifications. Availability and reliability analyses and models are prepared. The individual reliability and availability criteria are sufficient to support an overall HSI availability number which meets or exceeds the requirement that the mean time between forced outages caused by failures of HSI equipment is greater than fifty reactor operating years over the design life of the equipment. In addition, the overall HSI availability is such that the mean time between HSI equipment failures, which results in a reduction in plant availability, is greater than five years over the entire design life of HSI equipment.

4.1.3.2 Special Qualitative evaluations

The HSI is also designed so that failures or problems in one function or device will not propagate into failures of other functions or devices. The HSI is designed to prevent any single random failure of HSI functions or devices from causing a forced outage, challenging a safety system, spuriously actuating a safety system, or causing a condition which results in the need to declare one of the plant emergency classes.

The HSI control and monitoring systems are designed to protect against failures of HSI equipment degrading the performance of more than one major control or monitoring function. The functional and physical designs of these systems are segmented to inhibit the propagation of failures across major functions.

An evaluation of the vulnerability of the HSI to common mode failures is performed during the preparation of design and procurement specifications. After the detailed multiplexing system model is put in place, the HSI implementation process explicitly considers the potential for common mode failures and their effects in determining the architecture of the HSI. This process explicitly identifies failures that were considered, makes a qualitative assessment of the susceptibility to each failure, and identifies design measures taken to protect against these failures.

A preliminary evaluation of the reliability of the HSI is performed during preparation of the design and procurement specifications. After vendor selections are made, a detailed reliability evaluation is also performed to provide assurance that the final system design, including all modules, performs in accordance with system requirements.

4.1.3.3 Database Interactions with other HFE Tasks

The OER and BRR output may create issues necessary to track in the HFE Issue Tracking System (HFEITS). HFEITS captures issues and supporting information which need examination at every phase of the HFE process. This includes examination of items such as the following:

- Collect data to support evaluations of risk-important human actions and errors
- Help justify staffing needs
- Contribute to trade-off study evaluations
- Identify potential design issues
- Support potential design solutions

4.1.3.4 BRR/OER Database

The BRR/OER database, which consist of indexed shared files, provides predecessor design and operating experience documentation to the ESBWR Design Team, to identify and evaluate HFE issues. The BRR identifies system and function differences between the ESBWR and predecessor plants and design. Those differences are evaluated and resolved as inputs to the plant design. The HFEITS, tracks issues identified that require design, operating procedure, or training design.

The BRR/OER Database development defines the process for identifying, locating, classifying, and entering the BRR and OER documents. The database establishes the review and identification of documents for relevance, assigning attributes for database searching. The database is organized by attributes to support the design engineers and the HFE team.

4.1.4 Outputs

The OER activity is conducted and a results summary report is completed describing the personnel and methodology employed in the conduct of the activity and summarizing the OER outcomes and results.

5 RESULTS

5.1 Results Summary Report

The Operating Experience Review (OER) is performed in accordance with the MMIS and HFE Implementation Plan and it's requirements. The OER activity is conducted and a results summary report is completed describing the personnel and methodology employed in the conduct of the activity and summarizing the OER outcomes and results.

A complete results summary report is issued, which addresses the scope of section 1.2, summarizing the results of the operating experience reviews, including OERs of previous Nuclear Power Plant HSI designs, that identify human performance issues, and the HFE solutions that support human performance improvements. The report is broken down into the three areas of review:

1. Review of HSI equipment/technologies,
2. Review of nuclear and other industry summary documents, and
3. Personnel interviews.

For each issue, the report summarizes:

- A statement of the issue
- Issue source
- Potential human performance impact
- Classification
- Priority
- Human performance improvements

The results summary report is completed describing the following:

- The OER team members and backgrounds
- The scope of the OER
- The sources of operating experience reviewed and documented results
- The process for issue analysis, tracking, and review

5.2 Operating Experience and Lessons Learned Tracking

The results of the OER review activities are provided to designers by an Operating Experience Lessons Learned evaluation report. This report provides experience and lessons learned information classified by ESBWR systems for systems designers. The responsible design engineer determines appropriate resolutions to issues and enters the implemented resolutions in the operating experience and lessons learned tracking system. In cases where the resolution does not address an OER human factor issue or is not in compliance with HSI requirements, a potential human error discrepancy (HED) is written. The HED is entered into the HFE Issue Tracking System for traceable records to assure that the ESBWR implementation reflects the experience gained by the resolution of design problems in operating plants. The HED is evaluated on the basis of risk significance.

OER generated issues in the HFEITS represent Risk-Important Human Actions identified independently of the PRA analysis. These issues are compared with the PRA/HRA to provide an independent feedback check on the PRA and HRA analyses. The PRA and HRA analyses use various contexts, modeling techniques, assumptions, quality and quantity of data, etc., to define and quantify HAs. The PRA and HRA can be enhanced, by reviewing the issues entered into the HFEITS, to ensure they are also considered in the PRA and HRA modeling. For example, if there is a problem experienced by the operators in a previous similar design (as expressed through issues in HFEITS), it is expected that the corresponding PRA and HRA analyses would reflect the issue. If this is not the case, a review will probe the various contexts, modeling techniques, input assumptions, data, etc., as well as the validity of the HFEITS resolution of the issue to reconcile the discrepancy.

Risk-Important Human Actions are explicitly evaluated during the design process to assess their human error probability and identify features of the HSI and the plant that enhance human performance and contribute to a reduction in the assessed human error probabilities. The assessment of these risk important human actions is reported in the HRA basis documentation and the issues, problems, sources of human error, and the design elements that enhance human performance are provided for these special actions.

5.3 Applications of OER information

The HFE team maintains experience summary reports in the BRR/OER reporting system for use by the system designers. Each report is filed by attributes, which permit the reports to be classified by the ESBWR system and by the HFE issue. This permits sorting by the attributes to provide specific task context for analysis by the HFE team and responsible system design engineer. The results of the analysis help prioritize event and scenario selection for training and verification of the HSI design using simulations. Use of attribute sorting can show how issues have been resolved through design choices. OER generated issues can be used in Human Performance Monitoring to monitor the effectiveness of design choices during the ESBWR operational phase.

5.4 Periodic Reports

N/A

5.5 Technical Output Reports

N/A

Figure 1 HFE Implementation Process

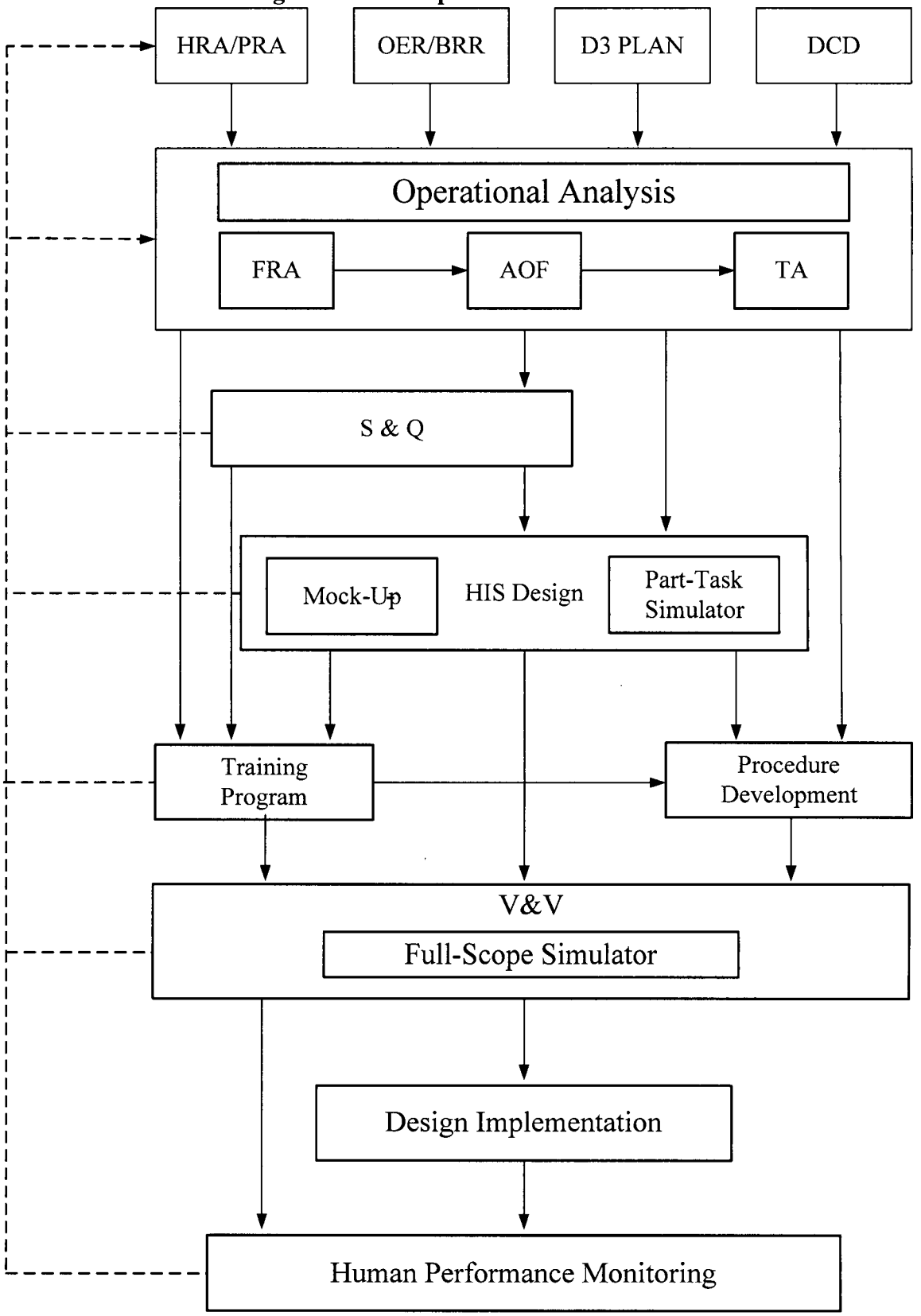


Figure 2 OER in the HFE Process

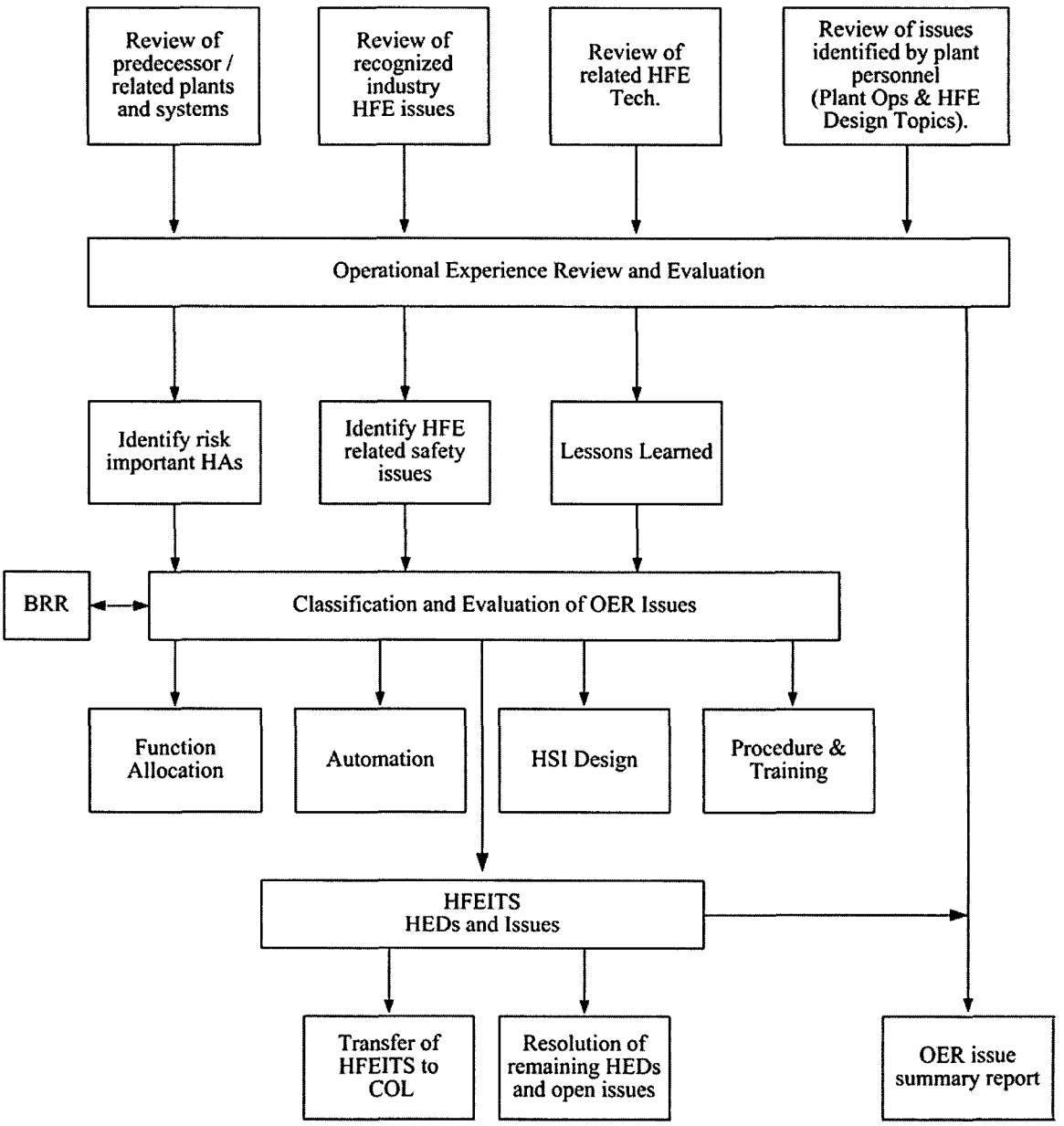
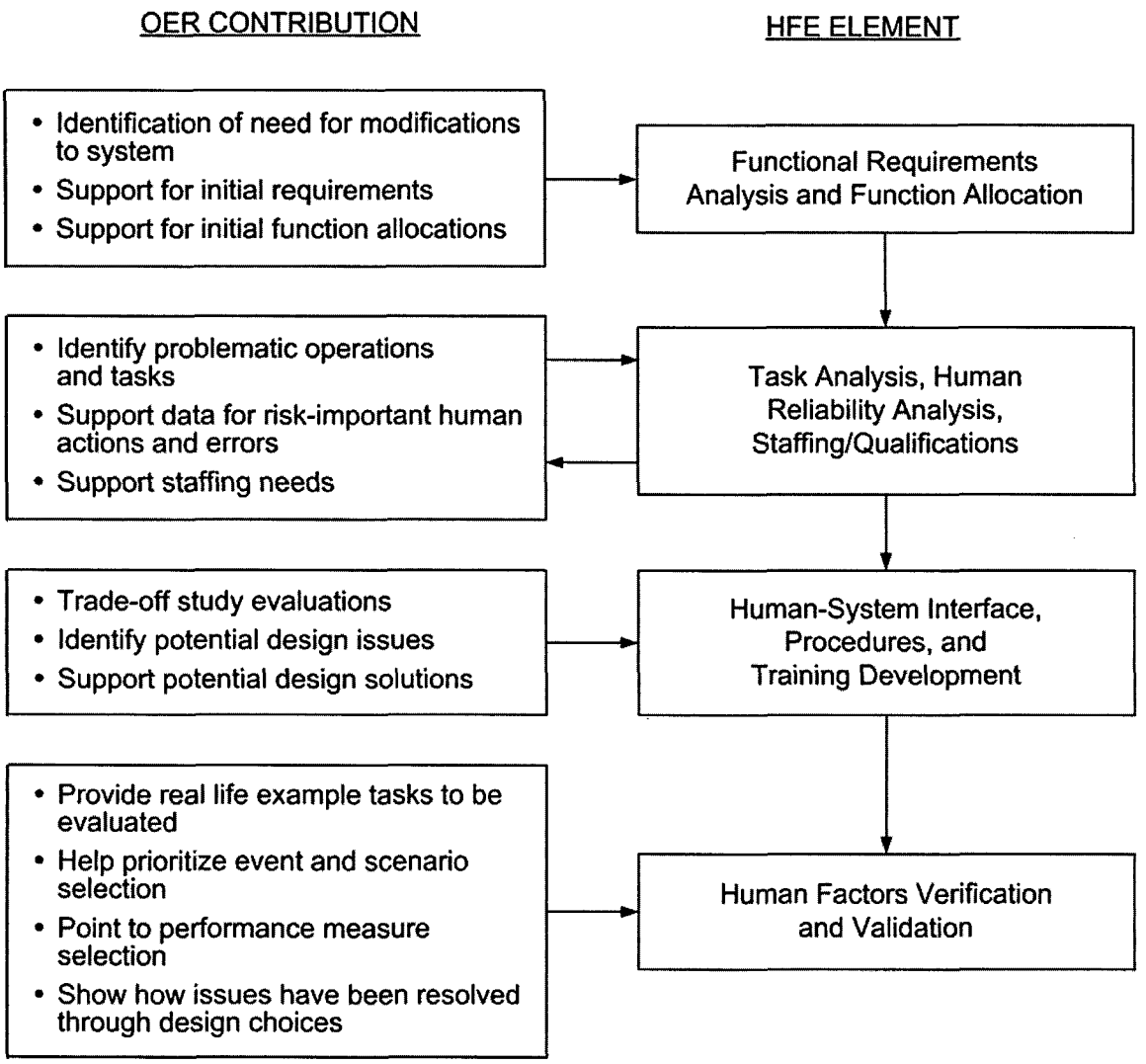


Figure 3 Role of OER in the HFE Process



Appendix A Example Identification of Human Interactions From Event Experience Related to BWRs

A.1 SUMMARY

In this example use of experience data human actions important for managing risk during outages at US boiling water reactors (BWRs) were analyzed using events for the period 1980-1991. This appendix describes the conditions and concerns for human actions in operational situations that have led to past events and generated lessons learned related to human factors improvement in indications, procedures, and alarm needs. Each item under the human interactions of interest represent issues that can be allocated to automated systems, shared or manual actions when considering new designs. By virtue of improvements in the ESBWR design, specific human interaction issues derived from the operating experience of older designs can be eliminated.

Several instances of loss of ability to maintain residual heat removal (RHR) during less than full-power operations have heightened industry concerns about a variety of abnormal conditions that can occur during shutdown. Events of concern include loss of reactor coolant system (RCS) inventory, loss of ability to remove decay heat, and loss of control of shutdown reactivity margins. In this example appendix the event experience from many plants was integrated using information from INPO's SEE-IN data base, Significant Operating Experience Reports (SOERs), Significant Event Reports (SERs), Operating and Maintenance Reports (O&MRs), and was augmented with Electric Power Research Institute (EPRI) reports, NRC information notices, generic letters and reports, and various vendor reports and utility studies described in section 3.

Shutdown operations are expected to have low risk significance; however, in light of the number of upset events that have occurred, it appeared warranted that further consideration of these conditions and their risks be studied. BWRs have experienced significant events during shutdown conditions. These have included unintentional drain downs of the reactor vessel to the suppression pool, loss of the residual heat removal system (RHRs), inadvertent plant heat up and pressurization, and unplanned criticality. Some of the BWR drain-down events have resulted in rapid decreases in reactor water level; however, in all cases, draining was stopped before any portion of the fuel was uncovered.

From 1965 to 1989, plants lost off-site AC power during shutdown on 74 occasions. Given the starting reliability of our two-train emergency diesel generator systems, the probability of losing

all AC power is about 10^{-3} to 10^{-4} per plant year. However--considering that maintenance outages of one or the other emergency diesel-generators occupy most of the overall plant outage schedule during refueling--in most of those 74 events, the plants were dependent on one diesel-generator train for restoration of AC power. The probability of losing all AC power in such circumstances is only one in a hundred. These events are directly related to losses of coolant inventory and could lead to boiling in the reactor core, if no operator recovery actions were taken. There are also numerous examples of RCS inventory loss and events, which could have led to inadvertent criticality.

Overall plant experience shows that the potential for high consequence events during less than full power operations should be considered. Abnormal equipment lineups, system malfunction due to equipment unavailability or human error, and the need to shorten maintenance times all play a role.

This appendix links events that have occurred during shutdown at nuclear power plants during the period 1980-1991 to specific human interactions. This study was prompted by the results of several risk studies at shutdown and many events that focused industry concern on the potential for high risk events during shutdown. This appendix covers individual conditions and concerns about human actions that can help a utility reduce shutdown risk. It is possible to divide the events into PWR and BWR issues: however, there are relatively few specific issues that are purely one or the other. Many events that appear to be only BWR-related have lessons applicable to PWRs and vice versa. An example of this is a BWR pressure vessel drain-down event, which on closer reflection has elements that can lead to problems in PWRs, if various uncommon system lineups occur.

The following sections address the functional events listed below:

Loss of RHRs function

Loss of off-site power

Loss of RCS inventory

Loss of fuel pool or reactor cavity inventory

Reduced reactivity shutdown margin

Fuel handling

A.2 EVENT SUMMARIES LOSS OF RHRS

A.2.1 EVENT TYPE: LOSS OF RHRS FUNCTION

CONDITION AND CONCERN: CAPABILITY TO MONITOR CRITICAL PARAMETERS

The ability to prevent and/or recover from loss of decay heat removal is greatly enhanced by the capability to accurately monitor critical primary system parameters (temperature, pressure, and level). There have been, for instance, several events that went unnoticed by operators because observed temperatures and flow were normal while pressure was increasing. Level indications can be in error by half a foot or more. Further, connection schemes, flow dynamics, entrapped air, or pressurization have been found to significantly affect all level instrumentation during operation with a lowered RCS inventory. These often contributed to the misdiagnosis of events and inappropriate operator response, which can exacerbate the problem. Another instrument-related problem is the limiting of operator information by the common practice of disconnecting instrumentation such as thermocouples in preparation for removing the RV head and for other operations commonly conducted during a refueling outage. A third problem has been vortexing of RHR pumps during operations with the reactor vessel head removed, when the water level in the RCS approaches the suction level of the RHR system.

REFERENCES: INPO SOER 88-3; NRC GL-88-17, IN 84-70, 85-75, 87-46; NSAC REPORT 52, 88; NUREG-1410

HUMAN INTERACTIONS OF INTEREST:

The following human factor issues were revealed during review of operational events:

- Key parameters important to the decay heat removal are not monitored and displayed prominently in the control room during shutdown periods. These include pressure, water level, temperature, and the position indications of some key motor-operated valves in RHR. Backup (independent) indications should be available for critical parameters.

- Air Entrainment of RHR pumps is not monitored (usually by pump motor current fluctuations), especially during situations (such as mid-loop) that are likely to lead to loss of RHR flow. Appropriate alarms (e.g., low RHR flow) need to be tested. The method for recovery from vortexing should be understood.

- Two independent level indication systems are not available. Problems encountered in previous events with pinching, binding, trapped air, etc. in tygon tubing level indicators need to be properly addressed in operations and maintenance activities. System conditions that affect these level indicators (e.g., vessel venting including effect of negative venting by eduction) need to be reviewed prior to changing decay heat removal configurations. Procedures should provide explicit guidance (including diagrams) for the routing/installation of temporary tygon level indications.

- Two independent indications of core exit temperature are not available at all times.

- The RHR system performance is not periodically monitored whenever an RHR system is in use to cool the RCS, particularly during sensitive evolutions. As an example. RHR operability should be periodically confirmed during each shutdown mode.

- Visible and audible alarm indications are not provided to indicate abnormal conditions in level, temperature, and pressure in the RHR system. Examples of RHR system indications include increasing RCS temperatures and fluctuations in current to the RHR pumps.

During the allocation process it is important to understand how these controlling functions are allocated (e.g., to human actions, partly automated or fully automated). It is likely that as in the past the most cost effective approach during the design is to allocate these functions to human actions, which may add to operational costs. For allocations to human actions, the designs should consider how the operators receive cues for actions and if the actions are in procedures and discussed in training.

A.2.2 EVENT TYPE: LOSS OF RHRS FUNCTION

CONDITION AND CONCERN: CONTINGENCY RECOVERY METHODS

In the early moments of an upset condition, the use of procedures based on automatic system responses and existing, redundant, safety-related systems and equipment would likely be the most practical method for handling decay heat removal. During a recent event: (1) there was incomplete implementation of existing analysis or guidance in procedures and training, (2) there were several instances of communications problems, and (3) the incident itself did not evolve according to the assumption upon which procedures were based. If an event develops in an unanticipated manner or key recovery systems are lost, various procedures can be implemented that will extend or restore core cooling.

REFERENCES: NSAC REPORT 146; NUREG - 1410; NRC GENERIC LETTER 88-17; INPO SOER 85-4

HUMAN INTERACTIONS OF INTEREST:

The following human factor issues were revealed during review of operational events. The existence of contingency plans and personnel training has been shown to be necessary to recover feedwater in the event of loss of RHR cooling. Although not always required by regulation, the best contingency plans for Boiling Water Reactors (BWRs) include:

- A small engine or DC-powered air compressor for plant air and diesel starting air

- A small backup pump from containment sump to refueling canal/cavity on loss of RHR during mid-loop operations with steam generator manways off

- Cross-connect the residual heat removal service water (RHRSW) systems to the RHR

- Connect the diesel fire water pump to the RHR system

- Supplement the pneumatic power supply to operate safety-relief valves

All backup equipment (especially connecting links such as spooling pieces) need to be available on-site, ready to perform, covered by procedures, and tested by a walk-through.

The NRC requires the plant staff to be familiar with recent significant events and training to be provided with the appropriate plant personnel prior to the plant entering a reduced inventory condition. SOER 85-4 recommended that contingency plans be tested and used in simulator training.

NOTE: It is important to keep in mind that backup equipment using temporary hookups is not the preferred short-term response to an event situation, and use of such equipment should be considered only in emergency situations.

A.2.3 EVENT TYPE: LOSS OF RHRS FUNCTION

CONDITION AND CONCERN: INADVERTENT CLOSURE OF RHR ISOLATION VALVES

Many events have occurred in which the RHR's heat removal capability has been lost because of an inadvertent closure of the RHR isolation valves. Inadvertent closure of these valves occurred shortly after initiating RHR operation, while decay heat was still high, and afforded the operator little time to correct the problem and restore decay heat removal before high temperature conditions were reached in the reactor vessel.

REFERENCES: INPO SOER 85-4 and 87-2; GE SIL-338; NSAC REPORT 52, 88 AND

HUMAN INTERACTIONS OF INTEREST:

A plant's ability to protect against inadvertent closure of RHR suction valves is strengthened by the following:

- Tagging procedures written to prevent leads from being improperly lifted (disconnecting power to relays causes isolation of RHR valves)

- Power supply output settings and motor generator over voltage relay settings that minimize breaker trips which cause RHR isolation valves to close

- Defective switch replacement, including switches subject to excessive drift, that are installed to isolate RHR suction valves in the event of excessive flow

- Procedures that address loose fuses or jumpers which, when touched or bumped, can cause RHR isolation valves to close

- Periodic calibration of pressure switches which provide the RV high pressure permissive signal to RHR isolation valves--Procedures should have adequate cautions to prevent inadvertent valve actuation during instrument calibrations.

- Only performing inboard RHR isolation valve pressure testing is with a pressure tap between the two isolation valves to indicate leakage of the outboard valve

- Deactivation of pressure interlocks that cause the RHR suction valves to close on loss of power to the interlock logic when steam generators are not available to remove decay heat

- Review of air-actuated RHR isolation valves to evaluate the loss of instrument air on these valves

- Disabling of the automatic RHR suction/isolation valve closure interlock that isolates the RHR system from the RCS when the reactor vessel head is removed-- In addition, plants that have adequate over pressure protection through the RHR system should disable the automatic closure interlock during all phases of RHR system operation.

A.3 EVENT SUMMARIES LOSS OF OFF-SITE POWER

A.3.1 EVENT TYPE: LOSS OF OFF-SITE POWER

CONDITION AND CONCERN: REDUNDANT SOURCES OF POWER

AC power is needed during shutdown conditions to maintain cooling to the reactor core, transfer decay heat to the heat sink, and restore containment integrity when needed. During shutdown conditions, technical specifications may allow sources of AC power to be taken out of service concurrently, increasing the chance for loss of AC power. Removal of sources of AC power concurrently is not prudent during mid-loop operation when the times to boiling in the core and core damage are significantly reduced. Since technical specifications for cold shutdown, refueling, and mid-loop operations are generally not based on a comprehensive safety analysis (including whether the single failure criteria should apply), plants should attempt to maintain as much additional margin beyond technical specifications as is consistent with efficient, low-risk outages.

REFERENCES: NRC IN 8442; NUREG-1410; INPO SERs 42-81 and 5-89

HUMAN INTERACTIONS OF INTEREST:

Power sources have been found to be most adequate when:

- Equipment taken out of service during an outage for maintenance is returned to service in a timely manner.

- An attempt is made to minimize the time at which the plant is at minimum technical specifications configuration for electrical power, and that maintenance activities are scheduled to preserve as much margin as possible, within reason.

- Modifications and work applicable to the above period are reviewed to ensure they do not affect existing operable power supplies (e.g., inadvertent relay actuation causing a loss of bus).

- Minimum technical equipment guidelines exist for conditions not covered by technical specifications in order to meet commitments of the site emergency, security, and fire protection plans.

- Plant personnel are at all times aware of the status of safety electrical systems and unusual interdependencies created due to new configurations.

- Testing of essential safety equipment is deferred if possible when plant is at or near the minimum technical specification limits.

A.3.2 EVENT TYPE: LOSS OF OFF-SITE POWER

CONDITION AND CONCERN: SWITCHYARD AND ELEC. EQUIPMENT ACTIVITIES

Of the 37 losses of offsite power events during shutdown (1965-1990), 18 were initiated as a result of human error. Most of these errors were associated with maintenance activities, e.g., switching errors, electrical maintenance and testing, and inadequate procedures. Inadvertent grounding of transformers has also led to loss of offside power. Working on energized equipment can also result in severe injury or loss of life.

REFERENCES: SER 17-88 and 36-87, NUREG 1410

HUMAN INTERACTIONS OF INTEREST:

Switchyard and electrical maintenance and testing activities can be effectively performed when:

- Special precautions are taken for activities near incoming and outgoing transmission lines and in the switchyard. Such precautions include caution signs near the activities (such as on the turbine roof) and special pre-job briefings.

- Periodic inspections of work areas and activities are made by utility safety and management personnel in order to detect developing hazards or improper work practices.
- Proper protection boundaries are established and all changes in work activities are considered prior to resumption of work. In addition entrance and time within protection boundaries are minimized.

- Only personnel qualified by training and experience are authorized to perform electrical equipment maintenance. License requirements for electrical equipment operation are enforced.

- Relay work on switchyard is included in a procedure and is reviewed and authorized by the site personnel. Procedures for switchyard work and testing are at least reviewed and authorized, if not controlled, by the site personnel.

- Training programs stress precautions such as the following:

  -- electrical equipment is assumed energized unless proven otherwise
  -- tag-out procedures
  -- resolution of any discrepancies in authorized work instruction
  -- proper use of safety equipment

- Procedures for working on high-voltage equipment that could cause major losses of power and/or personnel hazards are technically correct and reviewed for consideration of human factors.

- Maintenance activities on vital power lines are avoided to the extent possible during times that the reactor core cooling is especially sensitive to loss of power (e.g., mid-loop conditions) or when important electrical components (e.g., breakers, transformers) of parallel trains are out of service.

- The switchyard is not used as a storage or lay-down yard.

- Portable equipment such as air compressors or diesel generators should be located so that they can be refueled without entering the switchyard.

A.3.3 EVENT TYPE: LOSS OF OFF-SITE POWER

CONDITION AND CONCERN: ALTERNATE POWER (CROSS-CONNECTS/NON-SAFETY POWER/LOAD SHED)

In the event that off-site power is lost and emergency AC generator power is unavailable, the RHR system function will be lost and other safety functions such as closing the reactor containment building will be impaired. Alternate power sources can be used to help reestablish power to RHR and other safety functions, and various procedures to recover AC power and extend DC (battery) power can be implemented. Under worst case conditions, the inability to restore RHRS function may lead to core boiling in 1/2 hour or less, and core damage within a few hours. Temporary hookups and the availability of alternate AC power can greatly improve the situation, but only if the backup equipment is available on-site, ready to perform, covered by procedure, and has an installed hookup capability.

REFERENCES: NUREG - 1410; NSAC REPORT 146

HUMAN INTERACTIONS OF INTEREST:

Actions to align alternate power capabilities are strongly enhanced by the following:
A. Cross-Connect procedures for using alternate AC power sources are available and training has been conducted to eliminate unrevealed faults or triggering events.

- If "missing breaker" arrangements are used, personnel have the ability to locate and align the breaker and spooling components necessary to cross connect AC power.

- If "interlocks" are used, personnel can cross-connect AC power to the correct redundant trains of safety-related equipment, and administrative controls exist to prevent inadvertent cross connecting that would lead to faulty leg.

- Applicable breakers and bus locations are easily identified to allow switching operations of key components.

- Procedures require immediate action to reduce loads on DC buses (to prevent premature depletion of one of the DC systems) and to strip all nonessential loads (to extend the availability of DC power supplies).

- Equipment and tools have been staged for quick hookup, and operators and technicians were trained on the hookup procedures. Walk-through exercises have been performed to identify key switchgear and to verify that all tools are available, all fittings work, cable lengths are adequate, etc.

- Procedures have been developed to control the most probable alignments for cross-connecting power unit-to-unit or safety to non-safety buses. The procedures should discuss defeating interlocks, maximum load that can be supplied, and problems created because components such as transformers cannot be isolated.

B. Recover AC Power, Emergency procedures exist that:

- Diagnose and recover off-site power.

- Strip failed AC buses to ensure acceptability of the initial loading when AC power is reestablished.

- Diagnose and restart on-site emergency AC power.

C. Backup AC power Sources- Backup AC power sources such as small portable AC generators are provided to maintain DC power and supply power to installed systems. The generators should be readily accessible on-site, periodically tested, and have jumper cables tailored to the required applications.

A.4 EVENT SUMMARIES LOSS OF RCS INVENTORY

A.4.1 EVENT TYPE: LOSS OF RCS INVENTORY (BWRs)

CONDITION AND CONCERN: RPV DRAIN DOWN TO SUPPRESSION POOL

There are a number of potential inventory loss paths from the RPV through the RHR to the suppression pool when removing decay heat. A single mispositioned valve can initiate loss of inventory. Once initiated, the ensuing primary coolant inventory loss has the potential for uncovering irradiated fuel inside the reactor vessel.

A typical BWR has two or three automatic protective features that can prevent a core uncovery, but not all of these features are required to be available during cold shutdown or refueling operations. If these protective features were not in place, most inventory drain-down or pump-down events would terminate naturally at a water level that would expose about one-third of the core, based on the relative elevations of the core and vessel piping penetrations.

REFERENCES: INPO SOERs 87-2, 85-1; NRC IN 84-81; GE SIL-388; NSAC 88

HUMAN INTERACTIONS OF INTEREST:

Inadvertent RPV drain down to the suppression pool is minimized when:

- Steps in procedures account for loss of inventory during cold shutdown and guide the operator in using alternative water sources and pumps that are likely to be available during shutdown.
- Proper valve lineup is checked prior to placing the RHR system in service.
- Only limited and controlled bypassing of emergency core cooling system (ECCS) functions is Possible during shutdown in order to preclude automatic losses o coolant inventory.
- The automatic isolation function of the RHR (on low reactor pressure vessel [RPV] level) is operable during shutdown cooling for all potential drain paths, including idle as well as operating RHR loops.
- Valve interlocks exist to prevent both suppression pool and shutdown cooling suction valves from being open simultaneously (irrespective of which valve is initially open). Also, interlocks prevent opening of shutdown cooling (SDC) valves and full-flow test return valves at the same time.
- Caution tags are placed on the control room panel next to hand switches for controlling valves, which may cause inadvertent draining of the RV.

A.4.2 EVENT TYPE: LOSS OF RCS INVENTORY

CONDITION AND CONCERN: INADVERTENT TRANSFER OF COOLANT FROM RCS

Most large loss of coolant inventory events occur during shutdown. During shutdown periods, the RCS boundary enlarges because low-pressure systems such as the RHR are connected to the RCS. The

plant configuration's and activities during outages increase the possibility of a valve misalignment that can result in a loss of RCS inventory. Although primary pressure during cold shutdown is much lower than normal operating pressure, nevertheless core uncovering can occur in as little as 20 minutes since flow diversions during shutdown tend to be large. Recent events resulted in transfers of 9,500 gal. RCS water to the refueling water storage tank (RWST) and 110,000 gal. were sprayed into containment from the primary system and the RWST. Other transfers of coolant from the RCS result from improper adjustment of the RHR suction relief valve, or due to premature lifting and excessive blowdown of residual heat removal relief valves.

Human performance and procedures were contributing factors.

REFERENCES: NRC IN 90-55, 81-10, 86-74, and 84-81; NSAC Report 52 and 43; INPO SOER 82-4, and SER 75-81 and 5-90

HUMAN INTERACTIONS OF INTEREST:

Past events of loss of coolant from the RCS inventory have resulted from problems in three areas: (1) valve interlocks and valve-closing logic, (2) procedure adequacy, and (3) human performance. The following human factor issues were revealed during review and should be checked for this type of operational event.

- Maintain valve-closing logic and switch position on motor-operated valves in the closed position.

- Procedures clearly stipulate initial plant conditions for work.

- Potential adverse ramifications to operator error have been considered, and mitigation steps exist in operating and testing procedures. For example' written warnings and precautions are available to operators and technicians during evolutions such as containment spray pump testing.

- Emphasize proper sequencing of steps and restoration, especially for positioning of critical valves.

- Water level is closely and frequently checked during evolutions.

- The control room has adequate indication of actual valve positions for all valves capable of creating a loss-of-coolant accident (LOCA) via the RHRS (i.e., containment sump isolation valves, RHR-supplied containment spray isolation valves, etc.). Adequate low coolant level audible alarms are installed in the control room.

- Manual-locking devices, electrical interlocks, or motor-actuator breaker rackout is required on valves that must remain in a specified position, and consideration has been given to the need to restore valve operability in emergency situations.

- Applicable boration flow paths are verified prior to configuration changes for maintenance and testing.

Plant configurations during the outage should not exist where a single failure can result in a loss of RCS coolant inventory. If this configuration is expected to exist in the ESBWR design, administrative controls should be in place and new designs and retrofits should be considered to remedy this situation. Operator errors that have occurred frequently in the past include: opening suppression pool suction valve before closing shutdown cooling suction valve, intentional use of shutdown cooling for vessel level reduction, and inadvertent opening of test return, minimum flow and upper containment pool return lines.

A.4.3 EVENT TYPE: LOSS OF RCS INVENTORY (BWR)

CONDITION AND CONCERN: INADVERTENT SAFETY RELIEF VALVE ACTUATION, AUTOMATIC DEPRESSURIZATION SYSTEM (ADS)

The potential exists for reactor cavity drain down during refueling open main steam line plugs are not in place, as occurred in 1985. The possibility also exists for exposing nuclear fuel in the event of a rapid draining of the reactor cavity or spent fuel pool during a refueling outage because fuel assemblies, which are higher than the potential drain-down level, may become uncovered. While the opening of a safety relief valve (SRV) cannot result in uncovering the core, which is below the elevation of the main steam lines, SRV opening could be a serious problem if it occurred during fuel movement.

It is a common misconception that two-stage target rock safety relief valves will not open below 50 psig. Vendor testing has shown that these valves will open at pressures as low as 25 psig.

REFERENCES: INPO SER 38-85, SER 72~84, AND SOER 85-1

HUMAN INTERACTIONS OF INTEREST:

The following human factor issues were revealed during review of operational events. The allocation of actions to prevent inadvertent safety relief valve actuation should concentrate on ADS control systems maintenance and testing during refueling.

When possible maintenance and testing of the ADS system logic or support systems should not be scheduled during the fuel movement. When these activities are performed, procedures should require that the ADS initiation be disabled (by opening links in the logic or removing power from the valve solenoids) or that only one sub channel of logic be tested and reset at a time. Operators should monitor vessel water level during the activity and be prepared to stop the test and reset the logic should an inadvertent actuation occur.

- SER 72-84, Supplement 1, discusses the possibility of using main steam line plugs during the outages in order to prevent vessel down drain through safety relief valves or main steam isolation valves via the main steam lines. Main steam line plugs should be required to be installed whenever fuel or irradiated components are being handled.

- Care should be exercised when performing newly revised procedures for the first time to ensure no unanticipated failure or procedural error results in drain down.

A.4.4 EVENT TYPE: LOSS OF RCS INVENTORY (BWR)

CONDITION AND CONCERN: INADVERTENT PRESSURIZATION

Inadvertent pressurization events have occurred during cold shutdown operations in which the primary system pressure rose above prescribed limits. One 1989 BWR event resulted in a heat-up and pressurization to above 1,000 psig and showed that the potential existed to pressurize that plant all the way to the safety relief valve set-points, which would have caused a loss of RCS inventory. Other events have resulted from loss of natural circulation while shutdown during hydrostatic testing of the reactor pressure vessel and check valves and when RHR system isolation valves inadvertently closed. Over pressurization events can result in damage to low pressure piping and may exceed American Society of Mechanical Engineers (ASME) code limits for cold reactor vessels (e.g. nil-ductility limits), creating the potential for breaks in the reactor coolant boundary leading to a loss of RCS inventory.

REFERENCES: INPO SOER 82-2; NRC IN 84-74 and 89-73; NSAC REPORT 88; GE RICSIL-049; INPO SER 63-84 and 2-82

HUMAN INTERACTIONS OF INTEREST:

To avoid the possibility for inadvertent pressurization, consider the following:

A. Vessel Charging

When the RCS is closed and control rod drive pumps are being used to provide seal purge flow for the recirculation pumps, procedures require that vessel inventory is decreased (periodically) and water level is not increasing beyond that expected. Safety/relief valves (S/RVs) should be operable and maintenance on these valves deferred. The procedures should recognize that pressure limits for brittle fracture control are considerably lower than at normal operation and that relying on the spring opening set points of the S/RVs is not prudent.

- Operating procedures require that makeup flows to RCS (e.g., reactor coolant pump seal injection) are promptly isolated after RHR system inlet isolation valves close.

B. Hydrostatic Testing

- Protection from possible RPV over pressurization during hydrostatic testing should be provided. Typical provisions are recalibration of relief valves, operability of pressure vent valves from control room, etc.

- Adequate pressure instrumentation should be available and monitored in the control room. Testing of valves in instrument lines used to monitor RPV pressure should be allowed only after achieving full hydrostatic pressure.

C. Natural Circulation Core Cooling

- Reactor shutdown cooling procedure(s) should be developed that specify minimum natural circulation reactor water level (steam separator turnaround point plus water level instrumentation uncertainties). These procedures should require the following:

  -- When the reactor water level is above the minimum natural circulation level, operate at least one shutdown cooling pump to maintain the reactor water temperature specified for cold shutdown mode.

  -- When the reactor water level is at or below the minimum natural circulation level, operate at least one shutdown cooling pump in each loop flow to maintain the reactor water temperature specified for cold shutdown mode.

- Whenever feasible, shutdown cooling heat exchanger coolant (service water, reactor building closed cooling water) flow should be throttled to maintain the reactor coolant temperature prior to throttling shutdown cooling system flow.

- Reactor water level is maintained above the minimum natural circulation level whenever the forced cooling is unavailable. If the reactor water level is to be maintained (for any reason) at or below the minimum natural circulation level, periodic monitoring of vessel metal temperatures above and below the intended water level is initiated.

D. Outage Return

- Pressurization of the RCS during low-temperature operation (returning from refueling outage) is determined by the nil ductility limits of the reactor pressure vessel, particularly:

  -- starting reactor coolant pumps for venting or filling the RCS.

- Loss of instrument air resulting in letdown isolation, increased level followed by increased pressure.

- Starting an additional RHR pump

  -- inadvertent actuation of a high head ECCS pump

  -- over pressure protection system out of service

A.5 EVENT SUMMARIES LOSS of Fuel Pool/Reactor Cavity Inventory

A.5.1 EVENT TYPE: LOSS OF FUEL POOL OR REACTOR CAVITY INVENTORY

CONDITION AND CONCERN: REACTOR CAVITY SEAL FAILURE

Some loss of fuel pool water events can result in the entire contents of the reactor cavity being drained within a short period. In almost every spent fuel pool (SFP) was drained to the bottom of the fuel transfer canal or tube, the water level in the SFP would barely cover the fuel in the racks and typically would be below the suction piping for spent fuel cooling. Fuel being moved could be uncovered if the cavity drained. Fuel with less than 4-6 feet of water cover would result in high radiation levels in containment and a high radiation exposure hazard, including fuel being moved or suspended from manipulators.

REFERENCES: NSAC REPORT 129; INPO SOER 85-1, SER 9-86, 51-81, 72-84, 92-84, 9-86, 31-88; NRC IN 84-93, IE 84-03, 88-65

HUMAN INTERACTIONS AND LESSONS LEARNED OF INTEREST:

The probability of loss of fuel pool water events is reduced when:

- Procedures exist for dealing with high radiation levels in the SFP area while restoring level. The implications of loss of SFP level on radiation shielding and resulting personnel dose rates have been analyzed and addressed in the procedures.

- Abnormal operating procedures (AOPs) address methods for recovery from inadvertent pumping down or draining of the cavity and the fuel pool when the transfer tube is open), equipment loss by flooding, and potential system interactions. These procedures should also include alternate methods of SFP cooling and administrative controls on proper valve alignments for coolant makeup. Flooding of secondary containment should also be considered.

- The AOPs address all credible types of seal failures, including seal rupture and loss of air leading to displacement of reactor cavity seals. Other potential drainage paths are also analyzed such as the following:

  -- reactor cavity drains
  -- ventilation hatches from the drywell to reactor cavity
  -- residual heat removal shutdown cooling line
  -- recirculation system valves
  -- main steam isolation valves
  -- safety relief valves
  -- temporary nozzle dams installed in the steam generators

- During refueling operations, temporary instruments have been installed to warn operators of a seal failure with alarms for water level in the spent fuel pool and pressurization of the seal system.

- Seals are used which limit the leak size and the use of nozzle dams or main steam line plugs is restricted during handling of irradiated assemblies. Such seals have several

methods of protection (i.e., air pressure primary and seal mechanical design secondary) so that seal integrity is maintained on loss of air pressure.

- Measures to prevent and mitigate seal leaks have been also considered, such as submerged dams in the refueling cavity to ensure some minimum water above any fuel being transferred, flow restrictors that span the reactor cavity seal to reduce leakage flow, limiting the number of irradiated fuel assemblies in-transit or in the refueling cavity, etc.

- Rubber seals between gates receive preventive maintenance change outs to minimize seal failure, and are routinely checked for leaks and proper inflation pressure by operators.

- Check valves are monitored to ensure reverse drain down to the refueling water storage tank does not occur.

A.6 EVENT SUMMARIES - REACTIVITY SHUTDOWN MARGIN

A.6.1 EVENT TYPE: REACTIVITY CONTROL SHUTDOWN MARGIN

CONDITION AND CONCERN: UNPLANNED CRITICALITY/LOW TEMPERATURE

During periods of cold weather, the RCS water temperature can drift below the minimum value used to analyze reactor shutdown margin and fuel pool criticality. An event of this type occurred recently at BWR. Cold water injects positive reactivity to the core, decreasing the shutdown margin. This effect is more important in BWRs than in PWRs because the nominal shutdown, margins are smaller. Temperatures 10° C below the minimum temperature specification may reduce the reactivity shutdown margin by a factor of two. This effect applies to both the core and the spent fuel storage pool and may be especially important during fuel shuffling operation. (Note: Low coolant temperature may also increase the risk of a nil-ductility temperature event on the pressure vessel.)

REFERENCES: INPO SER 17-90

HUMAN INTERACTIONS OF INTEREST:

Based on past events, a utility analysis of cold weather shutdown margin should verify the following:

- Analysis for adequate reactor shutdown margin and margin to fuel pool criticality reflects the minimum temperature expected at the plant.

- Plant personnel are aware of the potential reduction in reactivity margin that cold cooling water presents and are cognizant of the effect of low temperature coolant on nil ductility temperature.

- Plant configurations that can result in lower coolant temperatures than expected address the potential for unplanned criticality (e.g., flow control values to heat exchangers being open greater than nominal).

- Refueling procedures do not allow fuel movement during times of lower than minimum temperature. Safety analyses used for fuel evolutions specifically consider low coolant temperatures.

A.6.3 EVENT TYPE: REACTIVITY CONTROL SHUTDOWN MARGIN

CONDITION AND CONCERN: INADVERTENT CONTROL ROD WITHDRAWAL OR MISPLACED FUEL

BWRs do not use soluble boron to control reactivity during refueling. Instead, reactivity margins are normally maintained by control rods and fuel loading controls. Shutdown margin can be significantly reduced during refueling by misplacing a few control rod blades or fuel assemblies. By loading fuel into an unrodded cell or by withdrawing a control rod from a fueled cell, the core may become critical. This could initiate cladding damage, release fissions products to the coolant, cause fuel damage with inadequate cooling and result in high radiation levels that could cause plant personnel exposure.

Due to the limited number of source range monitors, the way a core is loaded (spiral, U-shape, etc.) is important. An improper loading scheme can allow regions of the core to approach criticality without early detection by the monitor, greatly reducing the margin of safety. Complicated refueling procedures may also cause human performance problems that can erode safety margin. No generic guidance exists from either vendors or the NRC.

REFERENCES: SER 15-83, NSAC Report 129; NRC IE 89-03, IN 83-35

HUMAN INTERACTIONS OF INTEREST:

Past studies have shown that reactivity margins are best maintained by operators when:

- Fuel cells are loaded only after positive verification of control rod insertions, and no fuel is moved with any control rod drawn.

- Core status boards reflect current fuel, blade guide, and control blade status.

- Safety analyses performed for the purpose of safety and shutdown margin evaluation should include analysis of intermediate fuel assembly positions including fuel placed in other than its designated position. The placement and effectiveness of source range monitors need to be included in such evaluations.

- Control blades and fuel bundles are prevented from leaning. Movement of assemblies into and out of a cell is done in such a way that assures continued support and keeps the cell upright. Operators recognize that the number of available blade guides has a

large impact on fuel movement sequences, efficiency of refueling, and the shutdown reactivity of the core.

- Incore neutron monitors are checked for proper positioning during fuel shuffle.

- Procedures for the refueling sequence, typically prepared after the RPV head is removed and fuel leak testing is complete, are checked for completeness. Such last minute activities are more prone to stress type errors. Reactivity evaluation models can be used to check reactor shutdown margin to avoid fuel layouts where reactivity is too high.

- Fuel movement procedures could include guidance to reenter the procedure once a deviation occurs to limit the potential for double errors.

- The staff members responsible for refueling operations are trained in the procedures and understand the consequences of fuel movement under high burnup flux distributions, misplaced fuel and implications of higher enrichment fuel.

A.7 EVENT SUMMARIES FUEL HANDLING

A.7.1 EVENT TYPE: FUEL HANDLING

CONDITION AND CONCERN: FUEL TRANSFER EVENTS

Many past incidents involved planned handling and transport of new and irradiated fuel elements including (1) the dropping of fuel elements or fuel pins, (2) lodging or sticking of fuel assemblies in refueling equipment, and (3) improper loading or unloading of a fuel assembly in the core, causing it to topple and lean against other assemblies. Other incidents involved inadvertent or unexpected lifting of fuel assemblies or rod cluster control assemblies from the reactor core; often as the upper core support structure was being lifted. In some of these cases, an irradiated fuel assembly was subsequently dropped. Life threatening radiation exposures and the contamination of plant areas can result from such events.

REFERENCES: NSAC Report 129; INPO SERS 1-88, 21-86, 59-81, 31-83, 31-85, 5-86

HUMAN INTERACTIONS OF INTEREST:

Studies have concluded that fuel transfer operations can be improved when:

- An SRO is assigned fuel-handling responsibility and authority, with no other contingent responsibilities.

- Control rod insertion times are reviewed prior to fuel transfer out of the core as an indication of possible misalignment between fuel and reactor internals.

- Written procedures detailed plans and practice runs used, especially for unusual or infrequent handling operations. Refueling operations training is conducted prior to fuel transfer or movement of internals.

- All lifting operations involving fuel are done by tools designed to determine and carry the load. Personnel recognize that hoists surpassing their upper limit commonly results in dropped fuel assemblies.

- Operations with auxiliary hoists use direct, unobscured visual observation. Fuel movement stops when visual contact is lost. (Note: it is good practice to augment observations with underwater cameras, or use of observers with binoculars, etc.)

- Cavity and fuel storage water clarity is assured before fuel handling operations commence, and procedures require suspension of operations if pool clarity degrades.

- Pneumatically actuated fuel servicing equipment is checked out (underwater) prior to use. Manipulation of fuel servicing equipment is performed away from the core region whenever possible. Servicing equipment is checked for foreign material that could jam transfer mechanism. Testing is recognized as especially important after modifications to refueling equipment.

- A refueling safety manual exists which addresses specific safety provisions and precautions related to refueling operations. The manual addresses commonly identified problems. The safety responsibilities of contract and staff supervisory personnel are clearly stated. Warnings are included for potential problems. Personnel are trained for fuel transfer operations.

- Preventive maintenance is regularly performed on fuel-handling equipment, including inspection of internals lifting rig cable and magnetic particle/ultrasonic testing of lifting hooks prior to refueling operations.

A.8 REFERENCES

1 LOSS OF RESIDUAL HEAT REMOVAL FUNCTION

INPO Significant Operating Experience Reports

INPO Significant Operating Experience Report 84-7, *Pressure Locking and Thermal Binding of Gate Valves,* December 14, 1984.

INPO Significant Event Reports

INPO Significant Event Report xx-91, ~ *In Preparation - Inventory Draindown,* 1991.

INPO Significant Event Report 26-89, *Loss of Residual Heat Removal Capability Due To Common Mode Failure of Flow Control Valves,* October 4, 1989.
INPO Significant Event Report 11-89, *Inadvertent Introduction of Hydrogen Into The Instrument and Station Air Systems,* April 11, 1989.

INPO Significant Event Report 5-89, *Lack of Control of Testing Disables or Challenges Safety Systems,* March 3, 1989.

INPO Significant Event Report 36-88, *Loss of Residual Heat Removal Due to Misleading Visual Indication of Water Level,* November 30, 1988.

INPO Significant Event Report 35-87, *Non-lsolable Reactor Coolant System Leak,* November 12,1987.

INPO Significant Event Report 35-86, *Extended Loss of Shutdown Cooling due to Steam Binding of Shutdown Cooling Pumps,* October 24, 1986.

INPO Significant Event Report 31-86, *Loss of Residual Heat Removal Flow Due To Inadvertent Draining Of The Reactor Coolant System,* September 3, 1986.

INPO Significant vent Report 23-86, *Loss of Decay Heat Removal Due To Inadequate Reactor Coolant System Level Control,* July 3, 1986.

INPO Significant Event Report 17-86, *Loss Of Shutdown Co. , Flow,* May 27, 1986.

INPO Significant Event Report 79-84, *Loss Of Shutdown Cooling Due to Inaccurate Level Indication,* November 14, 1984.

INPO Significant Event Report 71-84, *Residual Heat Removal Pump Damage Caused By Operation With Suction Valve Closed,* October 2, 1984.

INPO Significant Event Report 60-83, *Loss of Residual Heat Removal (RHR) Cooling During Reactor Vessel Draindown,* August 30, 1983.

INPO Significant Event Report 59-83, *Residual Heat Removal (RHR) Pump Suction Valve Closure Due To Control Circuitry Design,* August 18, 1983.

INPO Significant Event Report 13-83, *Unplanned Radioactive Release and Loss of Shutdown Cooling,* February 25, 1983.

NSAC/INPO Significant Event Report 95-81, *Automatic Valve Closure Causing Loss of Shutdown Decay Heat Removal,* November 25, 1981.

NSAC/INPO Significant Event Report 91-81, *Steam Voiding in the Reactor Coolant System During Decay Heat Removal Cooldown,* October 6, 1981

NSAC/INPO Significant Event Report 89-81, *Level Instrumentation Oscillations Due To Reference Leg Flashing,* October 23, 19

NSAC/INPO Significant Event Report 87-81, *Inadequate Reactor Coolant System (RCS) Water Level Indication,* October 19, 198

NSAC/INPO Significant Event Report 78-81, *Erroneous Indication. Reactor Vessel Level Causes Loss of RHR,* October 1, 1981.

USNRC Reports

USNRC. Ornstein, Harold Dr., AEOD/C503 Case Study, *Decay Heat Removal Problems at US. Pressurized Water Reactors,* December 1 985.

USNRC Information Notices

USNRC Information Notice No. 90-61, *Potential for Residual Heat Removal Pump Damage Caused by Parallel Pump Interaction,* September 20, 1990.

USNRC Information Notice No. 90-26, *Inadequate Flow of Essential Service Water to Room Coolers and Heat Exchangers for Engineered Safety-Feature Systems,* April 24, 1990.

USNRC Information Notice No. 90-06, *Potential for Loss of Shutdown Cooling While at Low Reactor Coolant Levels,* January 29, 1990.

USNRC Information Notice No. 89-67, *Loss of Residual Heat Removal Caused by Accumulator Nitrogen Injection,* September 13, 1989.

USNRC Information Notice No. 88-36, *Possible Sudden Loss of RCS Inventory During Low Coolant Level Operation,* June 8, 1988.

USNRC Information Notice No. 87-51, *Failure of Low Pressure Safety Injection Pump Due to Seal Problems,* October 13, 1987.

USNRC Information Notice No. 87-23, *Loss of Decay Heat Removal During Low Reactor Coolant Level Operation,* May 27, 1987.

USNRC IE Information Notice No. 87-06, *Loss of Suction to low-pressure Service Water Pumps Resulting From Loss of Siphon,* January 30, 1987.

USNRC IE Information Notice No. 86-101, *Loss of Decay Heat Removal due to Loss of Fluid Levels in Reactor Coolant System,* December 12, 1986

USNRC IE Information Notice No. 85-75, *Improperly Installed Instrumentation Inadequate Quality Control and Inadequate Post Modification Testing,* August 30, 1985.

USNRC IE Information Notice No. 84-70, *Reliance on Water Level Instrumentation With a Common Reference Leg,* September 4, 1984.

USNRC IE Information Notice No. 83-88, *Air/Gas Entrainment Events Resulting in System Failures,* November 14, 1983.

USNRC IE information Notice No. ~ 9 *Degradation of Residual Heat Removal (RHR) System,* March 26, 1981.

USNRC IE Information Notice No. 80-20, *Loss of Decay H . Removal Capability at Unit 1 While in a Refueling Mode* May 8, 1980.

USNRC Generic Letters

USNRC Generic Letter No. 88-17, *Loss of Decay Heat Removal,* October 17, 1988.

USNRC Generic Letter No. 87-12, *Loss of Residual Heat Removal (RHR) While the Reactor Coolant System (RCS) is Partially Filled,* July 9, 1987.

USNRC IE Bulletins --

USNRC IE Bulletin No. 80-12, *Decay Heat Removal System Operability,* May 9, 1980.

USNRC NUREGs

USNRC NUREG-1269, *Loss of Residual Heat Removal System, Diablo Canyon, Unit 2, April 10, 19~7,* June 1987.

2 LOSS OF OFF-SITE POWER
INPO Significant Operating Experience Reports

INPO/NSAC Significant Operating Experience Report 80-5, *Potential Loss of Coolant Accident (LOCA) From A Single Electrical Failure,* September 23, 1980.

INPO Significant Experience Reports

INPO Significant Experience Report 11-88, *Inadvertent Disablement of The Automatic Start Capability For All Site Diesel Generators, May 6,* 1988.

INPO Significant Experience Report 25-85, *Emergency Diesel Generator Failed To Supply Emergency Bus Due To Non-emergency Trip,* June 3, 1985.

INPO Significant Experience Report 73-83, *Loss of All AC Power (Blackout),* October 27, 1983.

NSAC/INPO Significant Event Report 56-81, *Loss of Station and Reserve Auxiliary Power,* August 56, 1981.

USNRC Information Notices

USNRC Information Notice No. 91-22, *Four Plant Events Involving Loss of AC Power or Coolant Spills,* March 19, 1991.

USNRC Information Notice No. 90-25, *Loss of Vital AC Power With Subsequent Reactor Coolant System Heat-up,* April 16, 1990.

USNRC Information Notice No. 89-64, *Electrical Bus Bar Failures,* September 7, 1989.

USNRC Information Notice No. 89-16, *Excessive Voltage Drop in DC Systems,* February 16, 1989.

USNRC Information Notice No. 85-91, *Load Sequencers For Emergency Diesel Generators,* November 27, 1985.

USNRC Information Notice No. 88-75, *Disabling of Diesel Generator Output Circuit Breakers By Anti-Pump Circuitry,* September 16, 1988.

USNRC Information Notice No. 85-73, *Emergency Diesel Generator Control Circuit Logic Design Error,* August 23, 1985.

USNRC Information Notice No. 85-28, *Partial Loss of AC Power and Diesel Generator Degradation,* April 9, 1985.

USNRC Information Notice No. 84-69, Supplement 1, *Operation of Emergency Diesel Generators,* February 24, 1986.

USNRC IE Information Notice No. 84-42, *Equipment Availability For Conditions During Outages Not Covered By Technical Specifications,* June 5, 1984.

USNRC IE Information Notice No. 83-37, *Transformer Failure Resulting From Degraded InteMal Connection Cables,* June 13, 1983.

USNRC IE Information Notice No. 83-51, *Diesel Generator Events,* August 5, 1983.

USNRC IE Information Notice No. 83-17, *Electrical Control Logic Problem Resulting in Inoperable Auto-start of Emergency Diesel Generator Units,* March 31, 1983.

USNRC IE Information Notice No. 80-20, *Loss of Decay at Removal Capability at-- Unit 1 While in a Refueling Mode e,* May 8, 1980.

3 LOSS OF REACTOR COOLANT SYSTEM INVENTORY

INPO Significant Operating Experience Reports

INPO Significant Operating Experience Report 87-2, *Inadvertent Draining of Reactor Vessel to Suppression Pool at BWRs,* March 19, 1987.

INPO Significant Operating Experience Report 82-4, *Improper Alignment of Spray System To Residual Heat Removal System,* May 19, 1982.

INPO Significant Operating Experience Report 82-2, *Inadvertent Reactor Pressure Vessel Pressurization,* Apr. 28, 1982.

INPO Significant Event Report 7-91, *Failure to Control Valve Lineup Status Resulting in a Reactor Vessel Coolant Drain Down,* April 2, 1991.

INPO Significant Event Report 19-90, *Monitoring Plant Evolutions Using Inoperable Control Board Indications,* November 21, 1990.

INPO Significant Event Report 5-90, *Premature Lifting and Excessive Blowdown of Residual Heat Removal Relief Valves,* February 3, 1990.

INPO Significant Event Report 39-87, *Undetected Loss of Reactor Coolant Due To Release of Dissolved Gases,* December 29, 1

INPO Significant Event Report 4-86, *Internal Flooding of An Emergency Core Cooling System (ECCS) Pump Room,* January 6, 1986.

INPO Significant Event Report 37-83, Supplement 2, *Inadvertent Draining of Reactor Pressure Vessel To Suppression Pool,* October 9, 1985.

INPO Significant Event Report 37-83, *Inadvertent Draining of Reactor Vessel to Suppression Pool,* June 9, 1983.

NSAC/INPO Significant Event Report 85-81, *Inadvertent Discharge From Reactor Coolant System to Containment Sump,* September 25, 1981.

NSAC/INPO Significant Event Report 64-81, *Reactor Coolant Leak Due To Technician's Error,* August 14, 1981.

NSAC/INPO Significant Event Report 31-81, *Inadvertent Containment Spray,* April 29, 1981.

NSAC/INPO Significant Event Report 1-81, January 16,1981.

INPO Nuclear Network Entries

INPO Nuclear Network Entry WE 496, EAR TYO 90-005, *RPV Was Pressurized at Low Vessel Metal Temperature Condition During Refueling Outage,* March 1, 1990.

USNRC Information Notices

USNRC Information Notice No. 91-42, *Plant Outage Events Involving Poor Coordination Between Operations and Maintenance Personnel During Valve Testing and Manipulations,* June 27, 1991.

USNRC Information Notice No. 90-84, *Potential for Common-Mode Failure of High Pressure Safety Injection Pumps or Release of Reactor Coolant Outside Containment During a Loss-of-Coolant Accident,* October 4, 1990.

USNRC Information Notice No. 90-55, *Recent Operating Experience On Loss of Reactor Coolant Inventory While In A Shutdown Condition,* August 31, 1990.

USNRC Information Notice No. 90-05, *Inter-System Discharge Of Reactor Coolant,* January 29, 1990.

USNRC Information Notice No. 89-73, *Potential Over pressurization of Low Pressure Systems,* November 1, 1989.

USNRC Information Notice No. 87-46, *Undetected Loss of Reactor Coolant,* September 30, 1987.

USNRC Information Notice No. 87-38, *Inadequate or Inadvertent Blocking of Valve Movement,* August 17, 1987

USNRC Information Notice No. 87-25, *Potentially Significant 7t Problems Resulting From Human Error Involving Wrong Unit, Wrong Train, or Wrong Component Events,* June 11, 1987.

USNRC Information Notice No. 86-74, *Reduction of Reactor Coolant Inventory Because of Misalignment of RHR Valves,* August 20, 1986.

USNRC IE Information Notice No. 81-10, *Inadvertent Containment Spray Due To Personnel Error,* Mar 25, 1981.

Licensee Event Report 457-90002, *Transfer of Pressurizer Inventory to the Refueling Water Storage Tank Due To Procedural Deficiencies,* March 18, 1990.

GE RICSIL No. 049, *Inadvertent Vessel Pressurization,* January 5, 1990.

4 LOSS OF FUEL POOL OR REACTOR CAVITY INVENTORY

INPO Significant Operating Experience Reports

INPO Significant Operating Experience Report 87-2, *Inadvertent Draining of Reactor Vessel To Suppression Pool at BWRs,* March 19, 1987.

INPO Significant Operating Experience Report 85-1, *Reactor Cavity Seal Failure,* January 10, 1985.

INPO Significant Event Reports

INPO Significant Event Report 1-91, *Spent Fuel Pool Overflow Events.* January 4, 1991.

INPO Significant Event Report 17-90, *Reactor Coolant System Temperature Below Analyzed Limit for an Extended Time Period,* October 24, 1990.

INPO Significant Event Report 15-89, *Internal Flooding Resulting From Freeze Plug Failures,* June 9, 1989.

INPO Significant Event Report 31-88, *Reactor Cavity Seal Failure From Deflation and Inadequate Design,* October 27, 1988.

INPO Significant Event Report 3-88, *Inadvertent Draining of Reactor Vessels Due To Procedural Content and Usage Deficiencies,* February 12, 1988.

INPO Significant Event Report 7-87, *Pressurization of Vessel During Cold Shutdown,* March 19, 1987.

INPO Significant Event Report 4-87, *Pipe Break and Condensate Storage Tank Draining,* March 9, 1987.

INPO Significant Event Report 40-86, *Spent Fuel Pool Leakage,* December 24, 1986.

INPO Significant Event Report 8-86, *Inadvertent Drainage of Refueling Shield Tank,* February 24, 1986.

INPO Significant Event Report 41-85, *Containment Spraying Events,* September 19, 1985.

INPO Significant Event Report 38-85, *Reactor Vessel Partially Drained Due To Inadvertent Actuation of the Automatic Depressurization System (ADS) While in Shutdown,* August 12, 1985.

INPO Significant Event Report 92-84, *Partial Drain of Spent Fuel Storage Pool To Spent Fuel Shipping Cask Pit Due To Deflated Seal,* December 27, 1984.
INPO Significant Event Report 72-84, *Reactor Cavity Seal Ring Failure,* October 3, 1984.

INPO Significant Event Report 72-84, Supplement 1, *Reactor Cavity Seal Ring Failure,* April 18, 1985.

INPO Significant Event Report 72-84, Supplement 2, *Reactor Cavity Seal Failure,* February 13, 1986.

INPO Significant Event Report 63-84, *Over pressurization of Reactor Vessel During Cold Shutdown,* Aug. 30, 1984.

INPO Significant Event Report 46-83, *Inadvertent Initiation of Low Pressure Coolant Injection (LPCI),* July 1, 1983.

INPO Significant Event Report 2-82, *Cold Pressurization of Reactor Coolant System,* January 7, 1982.

NSAC/INPO Significant Event Report 76-81, *Loss of Primary Coolant To reactor Building Sump,* September 25, 1981.

NSAC/INPO Significant Event Report 61-81, *Inadvertent Spent Fuel Pool Overflow,* August 12, 1981.

NSAC/INPO Significant Event Report 51-81, *Spent Fuel Pool Watertight Gate Seals,* July 28, 1981.

USNRC Information Notice No. 89-73, *Potential Over pressurization of Low Pressure Systems,* November 1, 1989.

USNRC Information Notice No. 88-92, *Potential For Spent Fuel Pool Draindown,* November 22~ 1988.

USNRC Information Notice No. 88-65, *Inadvertent Drainages of Spent Fuel Pools,* August 18, 1988.

USNRC IE Information Notice No. 84-93, *Potential For Loss of Water From The Refueling Cavity,* December 17, 1984.

INPO Nuclear Network Entry OE 4629, *Low Level in Spent Fuel Pool due to Loss of Air to Transfer Canal Weir Gate Bladder,* June 4, 1991.

USNRC IE Bulletin No. 84-03, *Refueling Cavity Water Seal,* August 24, 1984.

5 FUEL TRANSFER

INPO Significant Event Reports

INPO Significant Event Report 15-91, *Fuel Mispositioning Events DL3 to Fuel Bundle Selection Errors,* June 11, 1991.

INPO Significant Event Report 10-88, *Fuel Assembly Lifted With Upper* InteMal, April 21, 1988.

INPO Significant Event Report 5-86, *Dropped New Fuel Assembly,* January 15, 1986.

INPO Significant Event Report 21-86, *Dropped Fuel Assembly,* June 16, 1986.

INPO Significant Event Report 31-85, *Inadvertent Fuel Bundle Movement,* June 27, 1985.

INPO Significant Event Report 31-83, *Irradiated Fuel Assembly Dropped From Fuel Handling Crane,* June 6, 1983.

INPO Significant Event Report 15-83, *Fuel Handling Error,* March 11, 1983.

INPO Significant Event Report 43-82, *Fractured Fuel Assembly Guide Tubes,* July 19, 1982.

INPO Significant Event Report 59-81, *Dropped Fuel Assembly,* August 11, 1981.

INPO Nuclear Network Entries

INPO Nuclear Network Entry OE 4167, *Fuel Assemblies Withdrawn With Upper InteMals,* October 5, 1990.

INPO Nuclear Network Entry OE 4112, *Fuel Assemblies Withdrawn With Upper Internals - Update to OE's 4167, 4177, and 4187,* October 26, 1990.

INPO Nuclear Network Entry OE 4113, *Fuel Assemblies Withdrawn With Upper lnteMals - Update to OE4167(message* replaced OE 4177), October 27, 1990.

INPO Nuclear Network Entry OE 4114, *Fuel Assemblies Withdrawn With Upper internals - Update to OE4167 and 4177(message* replaced OE 4187), October 27, 1990.

6 REACTIVITY CONTROL

USNRC Information Notices

USNRC Information Notice No. 83-35, *Fuel Movement With Control Rods Withdrawn At BWRs,* May 31, 1983.

USNRC Bulletins

USNRC Bulletin No. 89-03, *Potential Loss of Required Shutdown Margin During Refueling Operations,* November 21, 1989.

7. CONTROL ROOM MANAGEMENT

INPO Nuclear Network Entries

INPO Nuclear Network, WE 655 ENR PAR 90-061, Residual *Removal Flow Fluctuations During Drawing of Vacuum in the Reactor Coolant System,* September 19, 1990.

USNRC NUREGs

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

USNRC SECYs

USNRC SECY-90-326, *Quarterly Report on Emerging Technical Concerns,* October 4, 1990.