Advanced Reactor Human Factors (FIN E-2090)
Task No. 4: HFE Program Review Model
BNL Technical Report E2090-T4-3-1/95

HFE INSIGHTS FOR ADVANCED REACTORS BASED UPON OPERATING EXPERIENCE

James C. Higgins
Engineering Technology Division
Department of Advanced Technology
Brookhaven National Laboratory
Upton, New York 19973

January 1995

Prepared for

U.S. Nuclear Regulatory Commission
Washington, D.C.

Under Contract
DE-AC02-76CH00016

FIN E-2090

ABSTRACT

The NRC Human Factors Engineering Program Review Model (HFE PRM, NUREG-0711) was developed to support a design process review for advanced reactor design certification under 10CFR52. The HFE PRM defines ten fundamental elements of a human factors engineering program. An Operating Experience Review (OER) is one of these elements. The main purpose of an OER is to identify potential safety issues from operating plant experience and ensure that they are addressed in a new design.

Broad-based experience reviews have typically been performed in the past by reactor designers. For the HFE PRM the intent is to have a more focussed OER that concentrates on HFE issues or experience that would be relevant to the Human Systems Interface (HSI) design process for new advanced reactors. In support of that objective a list of pertinent OER issues and documents was provided as an appendix to the HFE PRM. This document was developed to expand that guidance and to provide a more detailed list of HFE-relevant operating experience pertinent to the HSI design process for advanced nuclear power plants. This document is intended to be used by NRC reviewers as part of the HFE PRM review process in determining the completeness of an OER performed by an applicant for advanced reactor design certification.

CONTENTS

CONTENTS

ACKNOWLEDGEMENTS

The author would like to gratefully acknowledge the NRC personnel that have contributed to the advanced reactor review work that has led to this report. They are the project engineers Clare Goodman and Garmon West, and additionally James Bongarra and Richard Eckenrode. These personnel are also acknowledged for their valuable comments on the draft versions of the report. The author would also like to thank John O'Hara of BNL for his many insightful comments and recommendations. The following BNL personnel contributed information that was used in selected portions of the report: Edward Grove, William Luckas, William Brown, Peter Kohut, and Charles Ruger. Additionally, Valerie Barnes provided excellent input on selected sections of the report. Finally, the author recognizes the excellent report preparation provided by Jeanne Madaia.

ACRONYMS

AFW	Auxiliary Feedwater
ASME	American Society of Mechanical Engineers
BWR	Boiling Water Reactor
CIV	Containment Isolation Valve
CV	Check Valve
CCW	Component Cooling Water
CR	Control Room
CRT	Cathode Ray Tube
CST	Condensate Storage Tank
DBA	Design Basis Accident
DC	Direct Current
EOP	Emergency Operating Procedure
ESF	Engineered Safety Feature
FC	Functional Centralization
HX	Heat Exchanger
HFE	Human Factors Engineering
HPCI	High Pressure Coolant Injection
HPSI	High Pressure Safety Injection
HPCS	High Pressure Core Spray
HSI	Human Systems Interface
HX	Heat Exchanger
IA	Instrument Air
I&C	Instrumentation & Control
IRM	Intermediate Range Monitor
LER	Licensee Event Report
LCS	Local Control Station
LOCA	Loss of Coolant Accident
LWR	Light Water Reactor
MFP	Main Feedwater Pump
MOV	Motor Operated Valve
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
OER	Operating Experience Review
PRA	Probabilistic Risk Assessment
PRM	Program Review Model
PWR	Pressurized Water Reactor
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RCIC	Reactor Core Isolation Cooling
RF	Radio Frequency
RHR	Residual Heat Removal
RV	Reactor Vessel
SART	Silence, Acknowledge, Reset, and Test
SBO	Station Blackout
TIP	Traveling Incore Probe
VPI	Valve Position Indication

1. INTRODUCTION

1.1 Background

Through the late 1980s and early 1990s, the Nuclear Regulatory Commission (NRC) has been preparing for and then actually conducting reviews of advanced reactor designs. The overall review and approval process for advanced reactors is presented in 10CFR52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants." As the initial designs were submitted, the NRC noted that in certain key areas, such as the control room and the instrumentation and control (I&C) systems, the designs were not sufficiently complete to support a conventional NRC review. There were several reasons for this, including: an advanced plant design had not yet been ordered for construction and may not be for several years, the nature of the technology design for both the control room human systems interface (HSI) and the I&C is currently evolving rapidly, and there is a desire not to lock the designs into what may soon become outdated or even obsolete. As a result, the NRC has adopted a review method that includes the review of the design process. There are other more substantive reasons for moving toward a design process review, which are discussed in some detail in NUREG-0711, Human Factors Engineering Program Review Model (1994.)

NUREG-0711 was developed to support the design process review for the 10CFR52 certification of advanced reactors. The PRM defines ten fundamental elements of a human factors engineering (HFE) program. An Operating Experience Review (OER) is one of these elements. The following paragraph provides some background for the use of an OER for a new reactor design.

The accident at Three Mile Island (TMI) in 1979 and other reactor incidents have brought to light significant problems in the actual design and design philosophy of nuclear power plant (NPP) HSIs. Many recommendations have been made as a result of these accidents and incidents, and utilities have implemented both NRC-mandated changes and additional improvements on their own initiative. However, the design changes were based on the constraints associated with backfits to existing control rooms (CRs) using early 1980s technology, which limited the scope of corrective actions that might have been considered; that is, more effective fixes can be made when designing a new CR with the modern technology typical of advanced control rooms.

The main purpose of the OER is to identify HFE-related safety issues. The OER provides information regarding the performance of fully integrated predecessor systems in a way analogous to full-mission validation tests, which provide information about the achievement of HFE design goals in support of safe plant operation for the integrated system under review. The issues and lessons learned regarding operating experience provide a basis for improving the plant design in a timely way, that is, at the beginning of the design process.

The resolution of OER issues may involve function allocation, changes in automation, system design, HSI equipment design, procedures, training, and so forth. Thus, problems and issues encountered in previous designs can be identified and analyzed so that they are avoided in the development of the current system or, in the case of positive features, to ensure their retention.

In the past broad-based experience reviews have typically been performed by reactor designers. For the PRM, the intent is to have a more focussed OER that concentrates on HFE issues or experience that would be relevant to the design of the new advanced reactors. In support of that objective a list of pertinent

OER issues and documents was provided as Appendix B to the HFE PRM. The current document was developed to expand on that information and to provide a more detailed list of HFE-relevant operating experience pertinent to the HSI design process of advanced NPPs

1.2 Development of Current Document

Currently, Element 2 of the PRM, "Operating Experience Review," lists in Criterion 3.4.1 (2), "Recognized Industry Issues," six categories of issues that should be addressed by an applicant for an advanced NPP. Appendix B of the PRM, titled "Operating Experience Review Issues," expands upon and provides example issues for the first four categories, namely: Unresolved Safety Issues/Generic Safety issues, Three Mile Island issues, NRC generic letters and information notices, and the Office for Analysis and Evaluation of Operational Data. It also provides an explanation of the HFE aspects of the issues. For the last two categories of Appendix B, low power and shutdown issues, and operating plant event reports, no example issues or details were provided. This document is intended to provide an expansion of the HFE issues in these last two categories of Appendix B.

In developing issues for inclusion in this document, an attempt was made to identify those HFE issues that could reasonably be construed to impact the HSI or the HSI design process. The HFE issues, that were identified, are wide-ranging and were derived from a variety of documents such as: NUREG reports, NUREG/CR reports, NRC Bulletins and Information Notices, industry reports, and Licensee Event Reports (LERs). Documents describing individual events, such as LERs, as well as more generic documents, such as NUREG/CRs, were used. Where available, documents summarizing recommendations in a particular area (e.g., shutdown operations) were reviewed. However, it is important to note that the review was not intended to exhaustively identify all issues pertinent to a specific design. Therefore, it is still necessary for a design certification applicant to conduct an OER tailored to their unique design.

The organization of this document reflects the operating experience issues identified and is intended to assist the reviewers in applying the information. Thus, sections 2 through 6 of the report present the operating experience categorized as follows: main control room, system-related insights, component-related insights, local control stations, and shutdown operations. Within these sections, there are presented issues related to such HFE areas as function allocation, HSI design, training, communications, and procedures. The document focuses on HFE items, but issues are often complex and sometimes the distinction between systems-related items and HFE-related items becomes blurred. For these type of issues, potential resolutions for both are identified.

A number of elements of the PRM must be addressed later in time than the OER effort. These include training, staffing, and procedures. Additionally, there is ongoing NRC work in all of these areas. Another HFE area of current NRC concern, where there is ongoing work is communications. As a result, these areas are addressed in this report but not comprehensively. Training issues are only noted where they may have an impact on the design.

The OER items are typically described in three parts: issue, potential resolution, and references. Sometimes when the discussion is short or when the issue and resolution are tightly intertwined, the presentation combines the issue and the potential resolution into one paragraph. Some of the resolutions are taken directly from recommendations of the reference documents, some are based on analyses of events by third parties (such as the NRC or industry organizations) and others are based on analysis by BNL. Relevant references are noted under each set of issues and resolutions. Section 7 provides a consolidated listing of all the references used for this report.

The events selected for analysis are typically representative of the issue being discussed, i.e., the references for the issue are not exhaustive and it should not be inferred that a referenced incident is the only instance of such an occurrence.

1.3 Use of Document by NRC Reviewers

As noted above, this document is intended to be used by NRC reviewers in performing reviews of advanced reactor submittals in the HFE OER area. Specifically, it addresses paragraphs B.5 and B.6 of Appendix B of the HFE PRM.

No requirements are implied by the information that is provided herein. However, as part of the OER, the applicant (usually the designer) is generally expected to have reviewed and considered the issues described herein. As a result of their review, applicants may identify whether each particular issue is relevant to the design, and if relevant, how the issue is (or will be) addressed. If the issue will be addressed at a later stage of the design process (e.g., post-design certification), then there should be appropriate tracking to ensure that this occurs. The NRC reviewer will typically verify that the applicant has appropriately considered operating experience by use of the PRM criteria and as supplemented by this more detailed document.

As an example, for a given issue the reviewers must first determine if the issue is applicable to the reactor design under review. Then they must determine if the applicant has appropriately addressed the issue in question. One way, but certainly not the only way, is through the implementation of the potential resolutions noted in this report. In fact for certain designs, the noted potential resolution may not be appropriate. The reviewer should also note if the applicant's solution is incorporated into the design or if it is merely deferred for later determination. In this case the item should be tracked in the applicant's tracking system.

2. MAIN CONTROL ROOM

2.1 System Integration

The issues noted in this section would likely all be addressed by a comprehensive HFE program as described in the HFE PRM. However, they are specifically noted here, in order to ensure that these somewhat global issues, which have created difficulties in the current generation of NPPs, are given appropriate attention.

Issue:

1. Integration of Information

Plant operations for routine transients (non steady-state plant evolutions), such as start-up, shutdown, and power changes, are sometimes difficult because of the need to integrate much information obtained from a variety of locations and the need to coordinate many operators. During unplanned transients, the volume of information immediately presented to operators can be overwhelming. Some examples of individual tasks that contribute to the difficulty are:

- Heat-up and cool down rate limitations (one operator is needed specifically to log and plot information)
- Control and verification of control element assembly (control rod) position

- Reactor coolant system letdown control

- Throttling of high pressure safety injection (or high pressure coolant injection) system flow during its emergency operation.

Potential Resolution (Issue 1):

Operators have noted that better display integration and increased automation may help them through these evolutions.

Issue:

2. Change in Control Modes

In transient situations operators often (especially after emergency actuation of systems) have to take manual control of many of the tasks that were automatically controlled (such as maintaining pressurizer and steam generator water levels). This change in control modes by itself is a challenge to the operators, and when added in the middle of a significant transient with its information integration problems noted above, is even more demanding.

Issue:

3. Memorization

Operators have to remember (memorize) their initial actions after a reactor trip, and are expected to accomplish them prior to procedural checks.

Potential Resolution (Issue 3):

One possible solution to the memorization issue is the development of appropriate operator aids for this purpose.

Issue:

4. Processed Information

Much information has to be calculated (sometimes mentally) by operators that could easily be provided directly with current technology. Examples are:

- Heat-up and cool-down rates,
- Primary system leakage, and
- Calculation of the approach to criticality ("1/m" plots).

Potential Resolution (Issue 4):

Provide computer-processed and validated data and calculated values needed by operators. This information should be provided in an integrated fashion with the full suite of controls and displays.

Potential Resolution (Issues 1-4):

Design of the main control room should be performed in an integrated fashion using a detailed process as described in NUREG-0711, and should specifically consider and address the issues noted above.

Issue:

5. Test and Maintenance

Test and maintenance activities have resulted in many LERs. In particular, surveillance testing can create problems as follows:

- There are a great many tests and the staffing required to perform them is large.
- Many tests require auxiliary operator support for day-to-day surveillance. (Many of these should be capable of being performed from the control room).
- Many tests produce spurious alarms that may confuse operators. Conversely, other tests deactivate alarms, making them temporarily unavailable to operators.
- Inadvertent actuation and isolation can and has occurred during testing.
- There is the potential to trip the plant and actuate emergency safety functions.

Potential Resolution (Issue 5):

Systems should be designed to be tested periodically without creating incidents. By appropriately considering test and inspection requirements in the design, some tests may be eliminated or automated, and other tests can be facilitated by the incorporation of test connections, switches, and installed instruments.

Reference (Section 2.1): System 80 Operating Experience Issues Based upon Interviews with System 80 Operators, BNL Technical Report E2090-T2-4-3/93, John O'Hara and William Luckas, Jr., March 29, 1993.

2.2 Alarms

This section relates to control room alarms. Considerable guidance relative to alarm systems has been incorporated into NUREG/CR-6105, Human Factors Engineering Guidelines for Review of Advanced Alarm Systems. The issues listed below are some of the main issues to arise consistently from operating experience.

Issues:

1. Avalanche of alarms

Perhaps the single biggest issue in the design of advanced alarm systems is the need to reduce the avalanche of alarms during plant upsets. The best method for achieving this goal has not been clearly resolved by research in the field. A number of possibilities and related issues are discussed in the two references noted below.

2. Prioritization of alarms

Prioritization is one way of addressing the issue of the avalanche of alarms. A prioritization scheme presents all alarms to the operator but codes them into priorities. Thus operators know which alarms the system considers important. A key question is the development of alarm prioritization schemes, which can prioritize alarms along several dimensions such as the overall importance to plant safety or the urgency of operator action. The selection of one or more of these dimensions will have a great impact on the alarm system's characteristics and, in all likelihood, operator performance.

3. Loss of power to annunciator panels

The loss of power to these panels could result in the loss of the operators' ability to respond to plant upsets, particularly if the operators are not aware of the loss. This is especially true with the emphasis on "black board" alarm displays.

4. Alarm displays

Alarm system research has identified multiple uses by operators of the alarm systems, namely: for alerting, for status monitoring, and for situation awareness. The selection of a display technology and display methods for the alarm system can significantly impact these multiple uses of alarm systems by operators. Both conventional fixed-location displays and the newer CRT-based displays have advantages and disadvantages.

5. Alarm controls

The specification of alarm system controls should also carefully consider the issues that surround them. For example, auditory features of alarm systems have been problematical and separate silence, acknowledge, reset and test (SART) controls are recommended. Further, the controls for advanced, computer-based alarm systems will become more complex and need attention.

Potential Resolution (Issues 1-5):

Carefully review the referenced documents with particular attention to the potential resolutions noted in the documents for the five key issues noted above. Others items from the cited reports may also be profitably considered.

For issue 3, alarm systems should have annunciation of loss of power to annunciator panels.

Regarding issue 4, the design of a virtual or CRT-based display for alarms should be certain to consider and address the possible disadvantages of this technique (e.g., loss of rapid detection and pattern recognition, decreased capability for situation awareness, unavailability to the entire crew, and added navigation workload.)

References (Issues 1-5): NUREG/CR-6105, Human Factors Engineering Guidelines for Review of Advanced Alarm Systems, J. O'Hara, et al.

Draft NUREG/CR, Advanced Alarm Systems and Human Performance, J. O'Hara, and W. Brown.

Issue:

6. Operator selectable alarms

In some instances, valves are routinely kept in a position so that they are ready for safety system actuation. An example is the HPCI and RCIC steam supply valves, which receive an automatic "open" signal on system actuation, but are nevertheless kept open. Inadvertent valve closure during normal operation has occurred in the past from operator failure to restore the valves after test or maintenance. This can be problematic in that: 1) the steam lines are not kept sufficiently warm (thus avoiding water hammer on system startup), and 2) the reliability of system actuation is decreased. However, it may not be desirable to have a permanent alarm that signals when the valves are not open.

Potential Resolution:

Consider an alarm for valves such as this in a "not open" state. Alternatively, the issue could be addressed by a low priority operator- selectable alarm to call attention to a component that may be out of its normal position. Alarm systems generally should have the flexibility for the operators to easily add alarms to a screen (for example) when a potentially deviant situation is identified that they need called to their attention.

Other obvious ways to help to address the concern are appropriate procedures and operator training related to valve positioning.

Reference: LER 50-254/80-006.

2.3 Controls and Displays

Issues:

1. Displays sometimes use engineering units which mean little to operators, e.g., "lbs-mass/hour" rather than percentage of full power flow.

2. Push button lamp replacement is problematic because the removal and replacement of the lens or bulb can sometimes cause inadvertent actuation.

3. On CRT-based displays, the operators are often restricted to the use of "prepackaged" displays and do not have enough capability to select parameters for display and trending.

4. Complex or poorly designed computer interfaces are supplied, as opposed to interfaces that are simple and "user-friendly."

5. The difficulty of upgrading computer systems can be a problem, even for relatively minor plant modifications.

6. Delays in computer responses are often a source of frustration for operators. Response time should be as short as possible and conform to HFE guidelines. A common specification for maximum delay time between screens is two seconds. This may be acceptable for routine computer processing, however during NPP transients it is too long and causes unnecessary operator frustration and delays in information processing.

7. Ensure that computer-based data points have a provision to indicate to the operators when the data for that point is invalid (e.g., point is out of scan.) This indication should appear on video displays and print-outs, as well as on the output of calculations where the data point is used.

Potential Resolution (Issues 1-7):

Ensure that the design process is thoroughly planned and utilizes appropriate guidance documents, such as NUREG/CR-5908 and NUREG-0700. Ensure that the design process takes into consideration the above issues raised by operators.

References: Items 1-6: System 80 Operating Experience Issues Based upon Interviews with System 80 Operators, BNL Technical Report E2090-T2-4-3/93, John O'Hara and William Luckas, Jr., March 29, 1993.

Item 7: LER 50-369/89-013.

Issue:

8. Ensure that there is adequate indication in the control room for trip status of important local equipment such as RCIC, HPCI, & AFW pump turbines.

References (Item 8): LER 50-397/87-002, LER 50-306/80-013, and LER 50-316/80-017.

2.4 Communications

NRC inspection reports and LERs from the late 1980s and early 1990s have highlighted many instances of communications errors and problems. There is currently ongoing work to classify and analyze these errors. This work is only in its early stages and thus this section does not include much information that will later be available. A few issues are noted here that pertain to the design of the communications systems.

Issues:

1. Communication Coverage

Effective and reliable communications between the control room operators and in-plant personnel is essential. Examples of some problems in this area follow:

1.1 Auxiliary operators often cannot be contacted in the plant due to their inability to hear pages from the control room (CR) since there are many hard-to-hear or dead spots in the plant.

1.2 Radio Frequency (RF) interference with communications due to inadequate shielding. A related interference issue to consider is communication radios causing unintended actuation of equipment.

1.3 Insufficient locations in the plant to "plug in" communications equipment.

2. Noise Interference

The noise level in the control room at some plants can be so high during transients that added stress for the operators is created and communication is difficult. Some examples of problems include:

- ESF actuated ventilation (especially 2 trains) is an additional annoyance
- High-speed conventional printers
- Alarms ringing constantly.

Operators can become so overloaded during complicated events that they sometimes don't silence or acknowledge the alarms.

Potential Resolution (Issues 1-2):

Ensure that communications requirements, above two issues, and past experience are considered at the design stage.

Reference (Items 1-2): System 80 Operating Experience Issues Based upon Interviews with System 80 Operators, BNL Technical Report E2090-T2-4-3/93, John O'Hara and William Luckas, Jr., March 29, 1993.

2.5 Procedures

As with the communications area above, procedure-related problems have often been identified in LERs and NRC inspection reports. The new area of computerized procedures is attempting to address some of the generic problems associated with current procedures. Both NRC and industry have ongoing projects related to computerized procedures. Some of the current issues are noted here.

Issues:

The following issues have been observed to be a problem with paper-based or hard-copy procedures in NPP operations.

1. Space for explanatory information is limited and the level of detail in procedure steps is fixed.

2. Non-linear information must be presented sequentially.

3. Irrelevant information regarding conditions that do not exist during a specific instance of procedure execution must be continuously displayed.

4. Cross-referencing introduces errors and delays in task performance.

5. Physical management of multiple procedures and place keeping during concurrent execution are awkward.

6. Maintaining the technical accuracy of procedures is particularly difficult in the paper medium. For example, a design change in a single component can invalidate every procedure that refers to that component. Similarly, a procedure revision that changes the step numbers in that procedure can invalidate every step in other procedures that cross-reference the changed procedure.

7. The task of using a paper procedure is typically not well integrated with the task to be performed. Unless the task itself is paper-based (e.g., performing manual calculations on a form), handling and reading a paper procedure while also performing the actions required to perform the task (e.g., placing jumpers) described in a procedure are typically incompatible.

Reference (Issues 1-7): Valerie Barnes, Pamela Desmond and Christopher Moore, "Preliminary Set of Review Criteria for Evaluating Computer-Based Procedures in Nuclear Power Plants," Performance, Safety and Health Associates, March 18, 1994.

Issue:

8. The physical handling and following of procedures has become a problem for some plants, due to the large number and complexity of procedures. Planning at the design stage can help alleviate some of these problems. Examples of difficulties are:

   a. Procedures are difficult to work with especially in the CR during a transient. There is no lay down area and portable carts have been used.

   b. Aids to follow procedures are needed.

Reference: System 80 Operating Experience Issues Based upon Interviews with System 80 Operators, BNL Technical Report E2090-T2-4-3/93, John O'Hara and William Luckas, Jr., March 29, 1993.

Potential Resolution:

(Issues 1-8) Procedures should be prepared with care utilizing an overall process that incorporates the features that are outlined in the HFE PRM (NUREG-0711) Element 8 and that considers the above operating experience issues.

2.6 BWR Shutdown

Issue:

During a reactor shutdown from an initial power of only 6%, that involved low decay heat levels due to a short operating history, operators allowed cooldown (due to small miscellaneous steam loads) to add excessive positive reactivity. Further, by not properly maintaining the power in the mid-range of the Intermediate Range Monitors (IRMs), a reactor trip occurred. Reviews of the event revealed that the transition from low power operation to hot shutdown conditions (via rod notch insertion) required the operator to monitor reactor pressure and cooldown rate and to maintain IRM levels on scale by adjusting the range switch settings, while simultaneously executing a prescribed and rather complex sequence of rod notch insertions. The arrangement and number of controls and displays makes it difficult for a single operator to accomplish all of this.

Potential Resolution:

Consider means to simplify and/or automate the nuclear instrumentation monitoring during startup and shutdown sequences. Consider the various types of startups and shutdowns when designing the controls and displays, in order to develop a panel that can support the operators in effectively accomplishing their function. Include special cases, such as noted above in procedures and operator training.

Reference: US NRC AEOD Report: Memo from J. Rosenthal to J. Novak dated September 20, 1991 with attached report, "Onsite Analysis of the Human Factors of an Event at Monticello on June 6, 1991 (Hi-Hi IRM Scram)."

3. SYSTEM-RELATED INSIGHTS

3.1 Flooding Concern

Issue:

Areas of NPPs, such as isolated rooms, often contain fluid systems with the potential for leakage and flooding.

Potential Resolution:

These areas should contain adequate drainage or sump pumping capability. Additionally, they should be provided with a high water level alarm in the control room.

Reference: LER 50-254/80-028.

3.2 Pressurizer

Issue:

A PWR pressurizer spray valve stuck open (unbeknownst to operators at the time,) causing a continued drop in RCS pressure to below that required by Technical Specifications. As a result, a plant shutdown was required in order to isolate the spray line.

Potential Resolution:

Ensure that there is sufficient information in the control room to determine status of spray to pressurizer. Also consider including a remote manually-operated isolation valve for the spray line into the plant design.

Reference: LER 50-336/80-020.

3.3 Loss of DC Bus

Issue:

Depending on the plant design, there are a number of potential problems associated with the loss of DC busses. Examples of consequent problems on loss of a DC bus are:

1. Partial loss of normal offsite power
2. Loss of control room annunciator power
3. Loss of power to indicators in control room
4. Loss of control power to various circuit breakers
5. Loss of power to computers and video display screens
6. Loss of some of the plant's automatic features, such as trips and interlocks
7. Trip of selected circuit breakers, such as reactor trip breakers

Potential Resolution:

The following considerations should be addressed:

I. Prevention of Loss of DC bus:

1. Ensure that DC power supplies are protected from inadvertent tripping or improper deenergization. Actions taken should include procedures for system breaker lineups, independent verification during certain maintenance activities, and control room indication of breaker position.

2. Provide for control of maintenance during operation to ensure the reliability of busses is maintained and extra monitoring is specified when some components (e.g., batteries or battery chargers) are out of service.

3. Provide annunciation for DC system ground faults.

II. Mitigation of Effects of Loss of DC bus:

1. Consider at the design stage the effects of a loss of a DC bus, giving particular attention to the effects that such a loss will have on the operators' ability to continue to effectively monitor and operate the plant (or shutdown the plant).

2. Where possible and appropriate, design redundant power supplies so that the loss of a single bus will not have significant and multiple consequences, such as listed in 1 through 7 in the Issue above.

3. Ensure that important trips and interlocks are still operable on loss of a bus.

4. Ensure that procedures adequately address the loss of a DC bus, recovery of lost busses, and the effects of re-energization of lost busses.

References: Report on the Millstone Unit 2 Loss of 125V DC Bus Event on January 2, 1981, by the Office for Analysis and Evaluation of Operational Data, November 1981, Report No. AEOD/C104.

LER 50-255/81-001, LER 50-285/82-017, and LER 50-333/81-082.

3.4 Automatic Trip of Condensate and Condensate Booster Pumps

Issue:

In BWRs during transient situations, vessel overfill can be a problem, causing main steam line flooding and possible damage. As a result, there exists a high reactor vessel (RV) level trip of injection systems such as HPCI, RCIC, Feedwater and HPCS. However, although the condensate and condensate booster pumps can also be used to feed the reactor vessel directly (at lower pressures), there currently is not an automatic trip of these pumps on high RV level.

Potential Resolution:

Consider providing a high RV level trip of the condensate and condensate booster pumps. For situations when the operators may not want to trip these pumps, this trip should have an operator-initiated bypass feature.

Reference: LER 50-397/87-002.

3.5 System Overpressurization

Issue:

During system restoration after maintenance during cold shutdown at a BWR, an incorrect valving sequence resulted in overpressurization of piping and damage to the test return line of the Condensate Storage Tank (CST) and Condensate Return Tank. This resulted in the spilling of about 275,000 gallons of slightly radioactive water.

Potential Resolution:

The design of new plants should consider operator valving errors in the specification of pipe and component design pressures, and the location of relief valves. Valve interlocks may also be used to prevent the simultaneous opening or closing of valves which may lead to overpressurization. Procedures that specify the sequence of valving are important in addressing this issue, particularly when necessary to prevent such overpressure conditions.

Reference: LER 50-341/86-045.

3.6 Feedwater System Control

Issue:

The control of PWR Feedwater Systems during startup and low power operations has been problematical. Operators have had difficulty in controlling the feedwater flowrate as necessary to maintain steam generator water levels. These problems are partially caused by the fact that the feedwater control valves and control systems are not designed to operate in the low flow regimes. Hence, operators are required to perform the difficult and sensitive operations manually with equipment that is not optimum. There has also been difficulty in the switchovers that occur in this time frame, namely: from manual to automatic control, from use of the auxiliary feedwater pumps to the main feedwater pumps, and from use of the small feedwater bypass valves to the main regulating valves.

Potential Resolution:

Consider provision of an automatic low flow or startup feedwater control system.

References: LER 50-344/83-02 Rev. 1, LER 50-368/84-004, LER 50-298/84-003, and LER 50-282/84-001.

3.7 Scram Discharge Volume

Issue:

On a BWR, when the scram discharge volume fills with water, insertion of the control rods is inhibited.

Potential Resolution:

Ensure that there is sufficient instrumentation to rapidly and reliably detect the presence of water in the scram discharge volume. Also ensure that the scram discharge headers are properly vented as all of the water received from a scram is removed.

References: NRC Bulletin 80-14, Degradation of BWR Scram Discharge Volume Capability.

LER 50-296/80-024.

3.8 Interfacing Systems LOCA (ISLOCA)

Issue:

Overpressurization of low pressure systems due to reactor coolant system boundary failures may result in rupture of low pressure piping. These sequences have the potential to lead to core damage with releases outside of containment. Some RCS boundary failures have occurred due to operator error. Important operator errors include valve alignment errors during transitions between operating modes. The operators also play an important mitigation role in these scenarios, particularly in break isolation. Section 3 of NUREG/CR-5102 provides a detailed history of ISLOCA events at PWRs. Also Section 3 of NUREG/CR-5124 provides a similar history of the ISLOCA events at BWRs.

Potential Resolution:

Important areas to consider in the protection against and mitigation of ISLOCAs include: the application of instrumentation to provide for the continuous monitoring of leaks, e.g., with pressure indicators, appropriate leak testing of boundary valves, use of pressure relief valves on the low pressure side, application of interlocks for boundary certain valves, personnel training, and development of emergency procedures to respond to an ISLOCA.

References: NUREG/CR-5102, Interfacing Systems LOCA: PWRs.

NUREG/CR-5124, Interfacing Systems LOCA: BWRs.

NUREG/CR-5928, ISLOCA Research Program Final Report.

IN 92-36, Intersystem LOCA Outside Containment, original and supplement 1.

NUREG-1463, Regulatory Analysis for the Resolution of Generic Issue 105: Interfacing System LOCA in LWRs.

3.9 Advanced Instrumentation & Control (I&C)

Issue:

Conventional I&C in NPPs has been associated with periodic failures, spurious reactor trips and plant transients, operator confusion on instrument failure and loss of power, extensive time and effort to accomplish testing, and difficulties in troubleshooting and repair.

Advanced I&C has the promise to address most, if not all, of the above issues, as well as to provide cheaper and more reliable equipment. Some of the positive features of advanced I&C currently available are: digital technology, multiplexed and fiber optic transmission, integrated circuits, automatic test features/equipment, self calibration, added redundancy, distributed microprocessors, fault tolerant design, improved response to and indication of individual instrument or circuit failures, ease of component repair via modular replacement, and automatic calculation of complex algorithms currently performed manually by operators (e.g., reactor power and heat balance determinations, heatup and cooldown rates, etc.) An example of monitoring for circuit failures that may be beneficial is the emergency diesel generator field flash circuit. As a result of the ease of installation and the small size of advanced I&C, one is able to increase redundancy and provide selective logic that can improve both reliability and safety. The design of the advanced I&C also lends itself to easily providing backup power supplies to important I&C busses. Self-testing and fault tolerance allow for rapid detection and repair of failures. These features also provide for reduced operator burden and confusion due to failed instruments and displays, through the use of synthesized and validated parameter displays.

The introduction of new technology naturally brings with it new problems and challenges. For example, although it is highly reliable, advanced I&C does have some peculiar problems, such as sudden failure and recovery, due in part to high susceptibility to electromagnetic interference. Also, because of the integrated nature of digital technology, the manual tracing of faults (even by trained technicians) can be physically difficult, time consuming, and cognitively demanding. Two difficult areas in digital I&C troubleshooting are symptom interpretation and test search (the selection of the proper tests to discriminate between many possibilities.) Automatic test equipment has been developed and used to overcome the

cognitive difficulties, the somewhat low reliability, and the time constraints associated with manual testing. In order to maximize the effectiveness of such new automatic equipment, careful attention must be given to the design of the operator interface for the equipment.

The introduction of advanced digital technology has also brought to forefront the importance of software programming for the new equipment, both during initial operation and during any modification. An effective verification and validation (V&V) plan for software that performs a safety function can help ensure acceptable design and continued successful implementation of the new equipment.

Potential Resolution:

The use of advanced I&C in design can result in many obvious advantages and can address many of the problems experienced in current NPPs due to conventional I&C. However, as with any new technology, one must also be careful not to introduce new (and, in this case, potentially more insidious) problems. Additionally, the new issues (noted above) associated with the advanced I&C should be considered and addressed in the design of advanced NPP HSIs.

References: Advanced Reactor SARs, Sections 7 and 18.

Crew System Ergonomics Information Analysis Center (CSERIAC) Report, Test and Maintenance of Digital Systems, CSERIAC-RA-93-015, by K. Klauer, et al.

Information Notice 93-57, Software Problems Involving Digital Control Console Systems at Non-Power Reactors.

LERs 50-346/85-008 and 50-440/91-009.

4. COMPONENT-RELATED INSIGHTS

4.1 Reactor Coolant Pumps

4.1.1 Seals

Failure of RCP seals has been an NRC Generic Issue for over a decade. This issue has concentrated primarily on PWR RCPs and includes: leakage and failure during normal operations and failure due to loss of seal cooling. Problems have also been identified with failure of BWR recirculation pump seals, indicating that this issue is not exclusively a PWR problem. Seal degradation and failure events have been and may continue to be aggravated by less than adequate HFE. A number of aspects of this issue can be addressed by HFE, in particular procedures and improved instrumentation.

Issues & Potential Resolutions:

1. Design Alternatives

This issue may be addressed by considering design alternatives which mitigate the problem and that obviate the need for other extensive and complicated fixes (such as below). One example is the use of canned rotor pumps that do not have seals.

2. Instrumentation

Current instrumentation has generally been found to be inadequate for evaluating off-normal and emergency conditions related to seals. Another concern is the ability of operators to use monitored parameters to infer premature degradation and incipient failure in multi-stage seal arrangements while avoiding false alarms. Thus the following Potential Resolutions are offered.

2.1 Ensure continuous monitoring capability of seal system data. Flow, temperature, and pressure data from the seal system should be continuously monitored and should be analyzed for seal performance trends.

2.2 Provide increased ranges on flow measuring devices so that off-normal values may be read as well as normal values. This may require the use of separate high and low range instruments.

2.3 Provide increased ranges on temperature measuring devices up to reactor coolant system temperatures.

2.4 Provide added pressure and temperature measurements, e.g., seal leakoff pressures, CCW return line pressure, seal cavity temperatures, differential stage pressures, and radial bearing temperature.

2.5 Provide added flow measurements, e.g., seal leakoff flows.

2.6 Provide for better alarming of the need for operator action.

3. Procedures and Operator Aids

3.1 Operator aids should be provided that allow the operator to appropriately trend RCP related parameters relative to seal performance criteria.

3.2 Emergency Procedure Guidelines, procedures, and training should be provided for a reasonable spectrum of seal failure events, such as: high seal leak-off flow, high seal temperature, high vibration, loss of seal injection, loss of seal cooling, station blackout, and RCP restart criteria. These procedures should incorporate the recommendations of RCP pump and seal vendors.

4. Functional Allocation

Isolation of seal leakoff lines on high flow, which has historically required operator action, should be evaluated as a candidate for automation since detection, recognition and action are time constrained. However, there are tradeoffs to automatic isolation which will need to be evaluated for each specific application.

References: NUREG/CR-4544, Reactor Coolant Pump Seal Related Instrumentation and Operator Response, W. Luckas, et al., December 1986, Executive Summary, Section 6, and Section A-1.

NUREG/CR-4948, Technical Findings Related to Generic Issue 23: Reactor Coolant Pump Seal Failure, C. Ruger and W. Luckas, March 1989, Section 4.3.2.2.

4.1.2 Pump Monitoring

Issue:

When RCP pump or motor components degrade they can eventually result in catastrophic failure of the pump or seals, if the pump is not stopped in time. Due to the location of the RCPs inside containment, detection of degradation must be accomplished through appropriate instrumentation. Large failures of the pump or seals can potentially result in a primary system LOCA.

Potential Resolution:

RCPs should have high quality vibration monitoring systems that can be used in the control room to detect incipient failures.

Reference: LER 50-255/84-021.

4.2 Auxiliary Feedwater Pumps

Issue:

1. Trip Status

In a case where the overspeed trip valve for the turbine-driven AFW pump turbine was inadvertently tripped and not properly reset, the control room operators were not aware of the inoperable status of the AFW pump.

Potential Resolutions:

Provide indication of latch reset/trip status for trip and throttle valve latching mechanism in the control room. Consider improved HFE at trip valve to identify and to prevent inadvertent tripping.

References: LER 50-306/80-013, LER 50-316/80-017, and LER 50-328/82-002.

Issue:

2. Steam Binding

AFW pumps have experienced steam binding resulting in pump inoperability. This has typically been caused by feedwater back leakage through the AFW discharge check valves, but also by leakage through complex pathways, working its way back to the AFW pump suction sources.

Potential Resolutions:

Provide temperature indicators and/or an alarms to monitor the temperature of the AFW piping. Ensure that procedures consider the possibility of back leakage and appropriately address it in their valve lineup sections.

References: IN 80-23, Loss of Suction to Emergency Feedwater Pumps.

LERS 50-261/83-016 and 50-368/80-018.

Issue:

3. Pump Driver Trips

Both turbine-driven and diesel-driven AFW pumps have experienced problems where the pump drivers have tripped due to sequencing type errors, making the pumps temporarily inoperable, when there was not a legitimate technical reason for the pumps to be inoperable. Examples follow:

Diesel-driven pump:

1. The diesel AFW pump had reached minimum operating speed (about 600 rpm) which closed the speed switch.

2. The stop signal was momentarily generated by the operator and was released before the diesel had come to a full stop.

3. When the control switch was allowed to go to "Auto After Stop," an auto start signal was present from loss of the MFP.

4. Due to the engine still being at greater than 40 rpm, the diesel starter motors were disabled and the diesel could not try to restart.

5. Twenty-five seconds after receiving the second auto start, the low lube oil pressure switch trip was enabled. This caused the engine to lockout due to the low oil pressure associated with the engine shutdown.

Turbine-driven pump:

After an auto start, operators erroneously tripped the AFW pumps. The steam-driven AFW pump had been restarted from the control room using the start valve which opened rapidly (less than 5 seconds) and caused the turbine to overspeed and trip. The auto start signal opens the trip and throttle valve on the initial auto start over a period of 20 seconds (by design, slow stroke time prevents the turbine overspeed). Until reset locally, the trip and throttle valve remains open when the pump is shutdown from the control room by shutting the start valve. When the faster acting start valve was used to restart the steam-driven AFW pump, the pump tripped on overspeed since the trip and throttle valve was already open.

Potential Resolution:

Consider providing AFW pump drivers and control systems such that operators can trip and restart the pumps in varying sequences without concern for spurious trips.

Alternatively, provide for clear procedures and training that outline the methods which operators must follow to ensure proper startup, tripping and operation of the AFW pumps.

Reference: LER 50-344/83-02, Rev. 1.

4.3 Inservice Testing of Pumps and Valves

Issue:

Current plants have had to devise complex test procedures that have often challenged operators and maintenance personnel due to designs that make testing very difficult, if possible at all.

Potential Resolutions:

The design for systems and components in new NPPs, should consider test requirements such as the inservice test requirements for pumps and valves per Section XI of the ASME Code. Specific Potential Resolutions in this area follow.

4.3.1 Installation of Test Connections for Leak Rate Testing and Check Valve (CV) Testing

1. When there are two CVs in series and both are required by safety analyses (e.g., for redundancy and single failure purposes), test connections should be installed between the CVs so that each can be tested separately.

2. Category A valves (per Section XI) and all containment isolation valves (CIVs) should have adequate test connections such that the valves can be safely leak rate tested to the requirements of ASME, Section XI and 10CFR50, Appendix J, without excessive operator realignment of systems and valves, temporary setups, operator radiation exposure, or potential for contamination.

4.3.2 Valve Position Indication

1. Consider external disk position indication for check valves that are required to be full stroke tested per Section XI.

2. Consider external position for other types of valves which may not have had such indication in the past, e.g., solenoid valves, and non-rising stem valves. All valves within certain categories should be considered for local VPI. See Section 5.3 for further discussion.

4.3.3 Capability for Full Stroke Testing of Valves

Ensure that single failure during stroke testing at power will not:

1. Cause a loss of safety system function.
2. Cause a loss of containment integrity.
3. Subject a system to pressures in excess of their design pressure.

4.3.4 Stroke Time Testing

Provisions should be made in the design to facilitate stroke time testing of Section XI Category A valves while the plant is at power, including rapid acting valves and control valves.

4.3.5 Pump Testing

1. Ensure that system design has sufficient flexibility to allow pump testing during plant operation. The system should allow flow to be varied so that a reference value of flow or differential pressure can be established for the test without major system reconfiguration. There should also be adequate installed instrumentation to run the necessary tests, including suction and discharge pressure, differential pressure, and flow rate. One means of improving flow instrumentation is to include flow rate instruments in the minimum flow recirculation line.

2. There should be installed pump vibration monitoring instrumentation to allow for trending and inservice testing of pumps.

References: NUREG-1482, Guidelines for Inservice Testing at Nuclear Power Plants, P. Campbell, November 1993.

American Society of Mechanical Engineers (ASME), Boiler and Pressure Vessel Code, Section XI, Rules for Inservice Inspection of Nuclear Power Plant Components.

10CFR50 Appendix J, Primary Reactor Containment Leakage Testing for Water-Cooled Power Reactors.

LER 50-400/91-008, Rev. 2.

4.4 Circuit Breakers

Issue: Breaker Lock-out

Under various conditions large circuit breakers may become locked-out due to protection system actions. These lock-outs were not always alarmed or indicated to the operators. An example is the safety injection pump breaker, which had a lock-out when an attempt was made to close the breaker with the hand switch in the presence of a trip signal. In this case there was no indication of the lock-out and the only means of clearing the condition was to remove and reinstall the fuses at the breaker or manually change the state of the relays.

Potential Resolution:

Circuit breaker lock-out conditions should be indicated and/or alarmed.

Reference: LER 50-327/80-040.

4.5 Spent Fuel Pool Seals

Issue:

Spent fuel pools have inflatable seals which are typically pressurized with instrument air. Loss of air pressure, among other items, can cause leakage or failure of these seals and subsequent draining of the fuel pool.

Potential Resolution:

Consideration should be given to alarms that detect failure of the seals, prior to an actual low level being detected in the spent fuel pool. Possibilities are low air pressure and water detected in areas outside of the fuel pool. This concern also applies to the refueling pool at PWRs and the reactor cavity during refueling at BWRs.

References: NRC IE Bulletin 84-03, Refueling Cavity Water Seal.

LERs 50-368/81-019, 50-361/84-060, and 50-213/84-013.

4.6 Heat Exchangers

Issue:

There have been numerous instances of biofouling in NPP heat exchangers (HXs), where various types of clams and mussels have grown inside of piping and particularly HXs. This occurs in open cycle cooling water systems and has caused sufficient fouling so that pressure drops have increased and flows have decreased. This in turn limits the ability to adequately cool components. Heat exchangers that have been affected include those for Component Cooling Water (CCW), Residual Heat Removal (RHR) and Emergency Diesel Generators.

Potential Resolution:

To ensure adequate cooling, sufficient instrumentation should be installed and test procedures established so that safety-related equipment, that depends on open cycle cooling water systems, can be adequately monitored for biofouling. This may include differential pressure and flow instruments on HXs and perhaps also on cooled components.

References: NRC Generic Letter 89-13, "Service Water System Problems Affecting Safety-Related Equipment."

NRC Generic Letter 91-13, "Generic Issue 130, Essential Service Water System Failures at Multi-Unit Sites."

LERs 50-325/81-032, 50-325/81-049, 50-311/83-013, and 50-296/84-001.

4.7 Power Connectors

Issue:

Power connectors have become accidently dislodged resulting in undesired transients. One example is power connectors for the feedwater control system, which led to a reactor scram.

Potential Resolution:

The design should ensure that connectors, whose disengagement could disable safety-related equipment or cause plant transients, cannot inadvertently be dislodged.

References: LERs 50-361/82-136 and 50-361/82-138.

4.8 Neutron Monitors

Issue:

A design flaw was identified in BWR Intermediate Range Monitors whereby the failure of a power supply fuse resulted in inoperability but was not annunciated nor did it create a trip situation from the detector output.

Potential Resolution:

Neutron monitoring system instruments should have supervisory monitoring circuits, so that either alarms are generated for internal component failure or the instruments are automatically placed in a safe (e.g., tripped) condition.

Reference: LER 50-263/86-016.

4.9 Instrument Air Dryers

Issue:

Due to a failure in the Instrument Air (IA) system filter, the desiccant from the dryer assembly carried over into the IA system and caused a failure of solenoid valves. This in turn caused a containment isolation valve (CIV) to become inoperable.

Potential Resolution:

Consider including in the design a means of detecting desiccant carryover. This may include instrumentation or a means for visual inspection or sampling.

Reference: LER 50-206/80-003.

5. LOCAL CONTROL STATIONS

A local control station (LCS) is an operator interface related to nuclear power plant 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.

5.1 General Considerations

Issue:

1. Use of HFE Principles in LCS Design

NUREG/CR-3696 and NUREG/CR-6146 give examples of many human factors issues observed in current plants at local control stations.

Potential Resolution:

LCSs serve as interfaces between the operators and the plant, similar to the work stations in the control room. Hence, the approach to their design should reflect the same HFE considerations given to the main control room, i.e., they should be designed using the same methods, standards, guidelines, and principles. The design of LCSs should be guided by the function and task analyses used to analyze the human role in the plant. It should be determined that functions to be performed at local control stations will not be compromised by human limitations and that the design of the LCS meets the needs of the operator for process information, means of effecting control, feedback on control actions, and an adequate working environment. In addition, the design of each LCS should be consistent with that of other local control stations and with the control room and should conform to *plant-wide* conventions regarding coding, labeling, information display, and operation of controls. Labeling should be well engineered, consistent, thoroughly applied throughout the plant, and appropriately designed to avoid wrong-unit/wrong-train type errors.

Issue:

2. Functional Allocation Considerations

In discussing problems that might be anticipated with future LCSs, Hartley et al. (1984) pointed to the allocation of an increasing number of local control functions to automatic or semiautomatic systems (as opposed to human operators). The difficulties they anticipated were the same as those that can arise from increasing automation in the control room, i.e., the potential loss of operators' situation awareness, and hands-on control skills (O'Hara, 1993) as their primary role becomes one of monitoring rather than controlling. A related observation was made during the plant visits undertaken for NUREG/CR-6146.

Potential Resolution:

Designers, procedure writers, and trainers must be aware of the potential problems inherent here and should take needed actions to minimize the development of such difficulties.

Issue:

3. HSI Consistency with Main Control Room

The reviews undertaken for NUREG/CR-6146 involved 11 site visits to observe LCSs. At all of the plants, operators in the control room had access to computer-based displays in addition to conventional displays. These displays provided high-level information, e.g., indications that represented an integration of several parameters, or the value of a set of parameters plotted over time. However, in only one of the plants were such displays available at the remote shutdown panel. This issue may become more significant in advanced plant designs, where control rooms are computer work station based, while LCSs (such as the remote shutdown panel) are based on conventional HSI. In such a plant, operators at remote shutdown stations might be forced to gather information about the status of the plant and the effectiveness of their actions by unaccustomed means.

Potential Resolution:

The designs of new or upgraded remote shutdown stations (and the content of related procedures and training programs) should ensure that the operator interface provides a level of support for operator actions comparable to that available in the control room and that potential error-likely situations are not introduced by negative transfer from the main control room to the LCSs.

References (Section 5.1): NUREG/CR-6146, Local Control Stations: Human Engineering Issues and Insights, Brown et al., March 1994.

NUREG/CR-3696, Potential Human Factors Deficiencies in the Design of Local Control Stations and Operator Interfaces in Nuclear Power Plants, Hartley et al., 1984.

NUREG-1192, An Investigation of the Contributions to Wrong Unit or Wrong Train Events, D. Persinko and A. Ramey-Smith.

5.2 Functional Centralization

Issue:

Functional Centralization (FC) refers to the manner in which the safety functions of LCSs are distributed throughout the plant. This embodies many of the systems engineering characteristics of LCSs and their functional organization. A plant with low FC has a wide distribution of safety functions on many local panels throughout the plant. Such plants also heavily use local control of individual components. A plant with high FC has all safety functions integrated into a single panel which contains all necessary controls and displays.

Functional Centralization affects human performance through its impact on such factors as communication workload, crew coordination, time to complete actions, and requirements for procedural complexity.

In NUREG/CR-5572, it was shown that centralization of functions at multifunction control panels was associated with large potential reductions in risk. The cost of backfitting this attribute into existing NPPs was found to be quite high, and the value/impact of the upgrade was therefore reduced. However, when considering such features at the design stage, it was noted that the values or risk reduction benefit would remain high while the costs would be much reduced.

Potential Resolution:

Consider providing the maximum reasonable amount of functional centralization for LCSs, particularly the remote shutdown panel.

References: NUREG/CR-5572, An Evaluation of the Effects of Local Control Station Design Configurations on Human Performance and Nuclear Power Plant Risk, O'Hara, et al., July 1990.

NUREG/CR-6146, Local Control Stations: Human Engineering Issues and Insights, Brown et al., March 1994.

System 80 Operating Experience Issues Based upon Interviews with System 80 Operators, BNL Technical Report E2090-T2-4-3/93, John O'Hara and William Luckas, Jr., March 29, 1993.

5.3 Valve Position Indication (VPI)

Issue:

NUREG/CR-6146 found that many manual valves, even those found to be the most risk significant manual valves, lacked local position indication. Without such explicit indication, the position of the valve is inferred from stem position (for rising stem valves) or determined by checking the valve in the closed direction. Both methods have potential problems, as discussed in the NUREG/CR. Operating experience review (OER) also identified incidents that were caused by poor or missing local VPI.

Valve manufacturers reported that the cost of providing a position indicator on a new valve was relatively small, whereas the costs of backfitting such indication on in-place valves would vary considerably and could be prohibitive. Thus, while adding position indication in an existing plant might only be feasible for a selected set of valves, it could be specified for many (or all) valves in the design of a new plant for relatively low cost. It should be noted that the nature of the position indication should be appropriate to the use of the valve.

Potential Resolution:

Incorporate local VPI into the design for valves in the design of a new plant. VPI should be included for all power operated valves, and most, if not all manual valves. If not all valves are provided with VPI, then there should be some clear criteria established to ensure that the more risk significant valves do get VPI.

References: NUREG/CR-6146, Local Control Stations: Human Engineering Issues and Insights, Brown et al., March 1994.

Special Report No. 87-10, Salem Generating Station, Docket No. 50-272, dated 4/13/88.

LER 50-397/87-002.

5.4 Miscellaneous Items

Issue:

1. Space at LCSs

Often there is not enough room for operators to work at the remote shutdown panel. In particular sufficient space for handling procedures is needed at the remote shutdown panel as well as at many other local panels.

Potential Resolution:

In task analyses and design of LCSs consider all activities that may take place at the LCS, including the need of the operators for adequate space and facilities.

Reference: System 80 Operating Experience Issues Based upon Interviews with System 80 Operators, BNL Technical Report E2090-T2-4-3/93, John O'Hara and William Luckas, Jr., March 29, 1993.

Issue:

2. Steam Generator Dump Valves

Manual operation of PWR steam generator atmospheric dump valves is often very difficult because of complicated manual arrangements, very high noise levels, high heat loads, and sometimes inconsistent valve operation with valves in close proximity to each other.

Potential Resolution:

Ensure that manual operation of the steam generator atmospheric dump valves is a design consideration and that the HFE issues noted above are addressed.

References: System 80 Operating Experience Issues Based upon Interviews with System 80 Operators, BNL Technical Report E2090-T2-4-3/93, John O'Hara and William Luckas, Jr., March 29, 1993.

NUREG/CR-6146, Local Control Stations: Human Engineering Issues and Insights, Brown et al., March 1994.

Issue:

3. Personnel Overexposure

Various areas of the plant have the potential for high radiation fields that could lead to personnel overexposure, therefore all p'ants have installed radiation detectors and alarms. Additionally, however, the malfunction of certain equipment can lead to very high radiation levels. This equipment includes incore instrument thimbles and traveling incore probes (TIP).

Potential Resolution:

There should be appropriate local warning devices (and perhaps also control room alarms) to alert personnel when equipment, such as TIPs and incore thimbles are not shielded and the potential exists for high radiation fields.

References: Events at Pilgrim Station on June 3, 1982 and August 18, 1984.

Information Notice 82-51, "Overexposures in PWR Cavities."

Information Notice 84-19, "Two Events Involving Unauthorized Entries into PWR Reactor Cavities."

LER 50-271/84-007 and LER 50-295/82-014.

Issue:

4. Emergency Lighting

Emergency lighting is required in the plant for personnel safety and for nuclear safety reasons. The two key nuclear safety areas requiring emergency lighting are the scenarios of 10CFR50, Appendix R, Section III.J and Station Blackout (SBO.) Operating experience has shown that NPPs have tended to pay less attention to the lighting requirements during an SBO scenario. A common practice is to depend on auxiliary operator use of flashlights. This can be a problem due to the potential unavailability of flashlights in an emergency and also because the physical use of one while operating equipment and communicating with the control room may be cumbersome.

Potential Resolution:

Ensure that the design incorporates fixed emergency lighting in all locations required by 10CFR50, Appendix R and wherever operations are needed during the plant's station blackout procedures.

Reference: NUREG/CR-6146, Local Control Stations: Human Engineering Issues and Insights, Brown et al., March 1994.

6. SHUTDOWN OPERATIONS

During the past decade the NRC and industry have become more aware of the need for maintaining the safety of operations during shutdown. Several events over this time period, as well as analytical studies, have highlighted the issues and the risks associated with shutdown conditions. This section addresses the HFE-related aspects of shutdown operations. The information here is taken largely from NUREG-1449, Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States. An effort was made to highlight those HFE areas which can be addressed at the design stage of a new NPP. This is particularly true for the areas of outage management, planning, training, and communications. Also, as noted earlier in this report, there is ongoing work in the NRC and industry in the areas of communications and procedures. Hence, these areas do not receive complete treatment here.

This section is one where the issues and the potential resolutions are merged into one discussion.

6.1 Outage Management and Planning

A well-planned outage is a major contributor to safety, while a poorly planned one could be a contributor to higher risk at shutdown. This aspect is primarily one for the operational phase of an NPP, however there are a few aspects that have pertinence to the design phase, which are included here.

Due to the importance of outage management and planning to shutdown operations, consideration should be given to the development of scheduling tools (e.g., computer-based outage planning and management aids, see Shore et al.) to assist in outage planning, scheduling, and management. Further, an interactive up-to-date PRA, which will allow a determination of the risk significance of removing selected pieces of equipment from service, would also serve to improve outage risk management.

6.2 Operator Training

Operators are often confronted with unfamiliar situations during shutdown operations. Training programs should be improved to appropriately consider the safety implications of these conditions. As an example, simulators should be able to model important shutdown operations to a greater extent than they currently do.

6.3 Procedures

Procedures are well known to be an important aspect of shutdown operations, as with other plant conditions. Appropriate human factors engineering in the control room and at local control stations that can assist in the implementation of such procedures should also be considered. Additionally, the effective integration of the various HSIs with the procedures is important. Particular areas of needing clear procedural coverage are:

1. Loss of residual heat removal (RHR) capability, including alternate means of removing decay heat such as gravity drain from refueling water tanks, safety injection, accumulators, or core flood tanks. Procedures should also address operator-induced loss of RHR and restoration of RHR upon loss.

2. Inadvertent draining of reactor vessel (RV): Procedures should contain adequate guidance for lowering RV level when operating in the RHR cooling mode. Also, there should be precautions against inadvertently draining the RV or draining the RV via multiple pathways at the same time. An example of inadvertent draining is having the RHR isolation valves (from the primary) open at the same time as other RHR valves, which can drain water from the RHR system. (LERs 50-265/87-010, 50-341/87-036, and 50-382/86-015).

3. Establishing and maintaining mid-loop (in PWRs) or other reduced inventory operations.

4. Use of temporary RCS boundaries such as freeze seals, nozzle dams, and thimble tube seals, including contingency plans in case of failure.

5. LOCAs during shutdown, including intersystem LOCAs and operator-induced LOCAs. See also item 3 under 6.5 below.

6. Rapid boron dilution accidents, such as the startup of an RCP in an idle loop that has a significantly lower boron concentration than the reactor.

7. Control of containment integrity during shutdown, including expeditious closure of open hatches and penetrations on a loss of RHR.

8. Fire protection during shutdown.

9. Loss of spent fuel pool cooling.

6.4 Instrumentation

Many current plants do not contain permanently-installed instrumentation to monitor the plant's safety status during shutdown. For new plants, instrumentation that appropriately supports shutdown operations should be considered for installation, including the following examples:

1. Two independent measurements of reactor coolant system level, including permanent instrumentation capable of measuring mid-loop conditions accurately. There should be adequate overlap between the RCS level instrument ranges to ensure complete coverage at all levels and to allow comparison between instruments as level changes ranges. Plants should avoid dependency on temporary, tygon tubing type level indicators, which have caused many problems in the past. Additionally, one should consider the potential inaccuracies of mid-loop level indicators that occur when one leg is vented to atmosphere and a slight pressurization of the RCS occurs. Instances have also occurred where the RCS was under a slight vacuum, resulting in level measurement inaccuracies. Additionally, there should be available displays and/or alarms of water level information in the refueling area while the reactor vessel head is removed.

2. Two independent measurements of core exit temperature.

3. Capability of continuously monitoring RHR system performance, including adequate alarm capability for out of specification temperatures, pressures, and flows.

4. Instrumentation containing appropriate ranges and accuracy to monitor shutdown conditions as well as power operating conditions.

5. Use of dedicated shutdown annunciators for special hazardous conditions that arise during shutdown (e.g., refueling cavity low level alarm). Also consider the use of trend displays during shutdown, such as RV level.

6.5 Equipment

The following are specific examples of equipment upgrades that would improve shutdown safety.

1. A containment equipment hatch design that allows for expeditious closure by operators when needed during a shutdown abnormal event. Similar provisions should be made for other containment penetrations that may be open during shutdown evolutions.

2. Improved human engineering of fuel handling equipment. Poorly-designed equipment, in the past, has led to fuel assembly drops and damage. This equipment should also be addressed by the HFE program.

3. Use valve interlocks to prevent overpressurization of low pressure piping and components, (LER 341/86-045).

4. Appropriate use of backup onsite power sources, such as emergency diesel generators, and portable power units.

6.6 Communications

An important aspect of maintaining normal shutdown conditions is adequate communications between the main control room and the rest of the plant. This includes areas where the following activities may take place: maintenance, testing, local operations, and monitoring activities. Effective communications are also very important during any abnormal events that occur during the shutdown period. Thus, when designing plant communications systems, care should be taken to consider shutdown operations. As noted earlier, there are ongoing NRC studies into communications errors and appropriate corrective and preventive actions needed.

References: Section 6, Shutdown Operations, was derived primarily from NUREG-1449, however a few items were added based on other references as noted below.

NUREG-1449, Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States, Final Report, September 1993 (all of Section 6).

IN 91-54, Foreign Experience Regarding Boron Dilution (Section 6.3.6).

E. Shore, et al., "Controlling Outage Scheduling: A Major Factor in Shutdown Risk Management," Nuclear Plant Journal, p. 32, September-October 1994 (Section 6.1).

LER 50-275/84-004 (Section 6.4.3).

LER 50-368/84-023 (Section 6.4.1).

7. REFERENCES

This section contains a consolidated and reorganized listing of the references mentioned throughout the report in the individual sections.

10CFR50 Appendix J, Primary Reactor Containment Leakage Testing for Water-Cooled Power Reactors.

Advanced reactor SARs.

American Society of Mechanical Engineers (ASME), Boiler and Pressure Vessel Code, Section XI, Rules for Inservice Inspection of Nuclear Power Plant Components.

Barnes, V., Desmond. P., and Moore C., "Preliminary Set of Review Criteria for Evaluating Computer-Based Procedures in Nuclear Power Plants," Performance, Safety and Health Associates, March 18, 1994.

Klauer, K. et al., Crew System Ergonomics Information Analysis Center (CSERIAC) Report, Test and Maintenance of Digital Systems, CSERIAC-RA-93-015.