

CA/TR-93-019-19

COOPER NUCLEAR STATION
TECHNICAL EVALUATION REPORT ON THE
IPE SUBMITTAL
HUMAN RELIABILITY ANALYSIS
FINAL REPORT

By:

P. M. Haas

Prepared for:

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Division of Systems Research

Draft Report December, 1993
Final Report May, 1995

CONCORD ASSOCIATES, INC.
Systems Performance Engineers

725 Pellissippi Parkway
Knoxville, TN 37932

Contract No. NRC-04-91-069
Task Order No. 19

ENCLOSURE 4

960220092 960214
PDR ADOCK 05000298
P PDR

TABLE OF CONTENTS

| | |
|---|----|
| E. EXECUTIVE SUMMARY | 1 |
| E.1 Plant Characterization | 1 |
| E.2 Licensee IPE Process | 1 |
| E.3 Human Reliability Analysis | 2 |
| E.3.1 Pre-Initiator Human Actions | 2 |
| E.3.2 Post-Initiator Human Actions | 2 |
| E.4 Generic Issues and CPI | 3 |
| E.5 Vulnerabilities and Plant Improvements | 4 |
| E.6 Observations | 4 |
| | |
| 1. INTRODUCTION | 6 |
| 1.1 HRA Review Process | 6 |
| 1.2 Plant Characterization | 6 |
| | |
| 2. TECHNICAL REVIEW | 8 |
| 2.1 Licensee IPE Process | 8 |
| 2.1.1 Completeness and Methodology | 8 |
| 2.1.2 Multi-Unit Effects and As-Built, As-Operated Status | 8 |
| 2.1.3 Licensee Participation and Peer Review | 9 |
| 2.2 Pre-Initiator Human Actions | 10 |
| 2.2.1 Pre-Initiator Human Actions Considered | 10 |
| 2.2.2 Process for Identification and Selection of Pre-Initiator Human Actions | 10 |
| 2.2.3 Screening Process for Pre-Initiator Human Actions | 11 |
| 2.2.4 Quantification of Pre-Initiator Human Actions | 11 |
| 2.3 Post-Initiator Human Actions | 13 |
| 2.3.1 Types of Post-Initiator Human Actions Considered | 13 |
| 2.3.2 Process for Identification and Selection of Post-Initiator Human Actions | 14 |
| 2.3.3 Screening Process for Post-Initiator Response Actions | 15 |
| 2.3.4 Quantification of Post-Initiator Human Actions | 15 |
| 2.3.4.1 Consideration of Timing | 17 |
| 2.3.4.2 Other Performance Shaping Factors Considered | 17 |
| 2.3.4.3 Quantification of Recovery Actions | 19 |
| 2.3.4.4 Consideration of Dependencies | 20 |
| 2.3.4.5 Treatment of Operator Actions in the Internal Flooding Analysis | 22 |
| 2.3.4.6 Sequences Screened Out Due to Credit for Recovery Actions | 22 |
| 2.3.4.7 Treatment of Operator Actions in the Level 2 Analysis ... | 22 |
| 2.3.4.8 GSI/USI and CPI Recommendations | 23 |

Table of Contents (continued)

| | | |
|---------|--|----|
| 2.4 | Vulnerabilities, Insights and Enhancements | 23 |
| 2.4.1 | Vulnerabilities | 23 |
| 2.4.2 | IPE Insights Related to Human Performance | 23 |
| 2.4.2.1 | Insights from the Level 1 Analysis | 23 |
| 2.4.2.2 | Insights from the Level 2 Analysis | 25 |
| 2.4.3 | Human-Related Enhancements | 25 |
| 3. | CONTRACTOR OBSERVATIONS AND CONCLUSIONS | 27 |
| 4. | DATA SUMMARY SHEETS | 29 |
| | REFERENCES | 30 |

E. EXECUTIVE SUMMARY

This Technical Evaluation Report (TER) is a summary of the documentation-only review of the human reliability analysis (HRA) presented as part of the Nebraska Public Power District submittal of the Cooper Nuclear Station (CNS) Individual Plant Examination (IPE) to the U.S. Nuclear Regulatory Commission (NRC). The review was performed to assist NRC staff in their evaluation of the IPE and conclusions regarding whether the submittal meets the intent of Generic Letter 88-20.

E.1 Plant Characterization

CNS is a single-unit General Electric (GE) boiling water reactor (BWR-4) plant, with a Mark I containment. The unit is rated at 2381 MWt and 778 MWe (net). Commercial operation began in 1974. Similar units in operation are Brunswick and Hatch. Distinctive design features cited by the front-end reviewer include several, such as service water cross tie capability and fan coolers in the diesel generator ventilation system, which have associated human performance implications. A significant design feature cited by the front-end reviewer which tends to decrease core damage frequency and has associated operator action is the ability to use the control rod drive (CRD) pumps for shutdown cooling. Two CRD pumps provides sufficient injection capability for core cooling during shutdown if all other cooling systems are lost. A significant human performance impact cited by the licensee is the upgrade of Emergency Operating Procedures (EOPs) to be consistent with Rev. 4 of the BWR Owners Group EPGs. The submittal notes in particular two risk-significant improvements associated with the upgraded procedures: (1) improvements in the directions to switch the Emergency Core Cooling System (ECCS) pumps to the emergency condensate storage tanks, and (2) procedures for venting. Operator failure to depressurize, either by incorrectly inhibiting the automatic depressurization system (ADS), or failure in manual depressurization using the safety relief valves (SRVs) was identified by the licensee as a significant contributor to core damage frequency (CDF) for CNS.

E.2 Licensee IPE Process

The HRA process addressed both pre-initiator actions (performed during maintenance, test, surveillance, etc.) and post-initiator actions (performed as part of the response to an accident). Pre-initiator actions considered included both restoration errors and miscalibration. Post-initiator actions included both response-type and recovery-type actions. The primary HRA techniques employed to quantify human error included the Accident Sequence Evaluation Program (ASEP) HRA procedure (Ref. 1) for pre-initiator actions, and the time reliability correlation (TRC) approach of Daugherty and Fragola (Ref. 2) for post-initiator actions. Plant-specific performance shaping factors and dependencies were considered to some degree in both pre-initiator and post-initiator analyses. Human errors were identified as significant contributors in accident sequences leading to core damage, and human-performance-related enhancements were identified and credited in the IPE/HRA or cited for future consideration. Licensee staff with knowledge of plant design, operations and maintenance had significant involvement in the HRA process. Procedures reviews, interviews with operations staff, and plant walkdowns helped assure that the IPE represented the as-built,

as-operated plant. An independent review of the HRA performed by and independent contractor and in-house staff helped to assure appropriate use of HRA techniques.

E.3 Human Reliability Analysis

E.3.1 Pre-Initiator Human Actions.

The HRA addressed pre-initiator human actions in maintenance, test and surveillance tasks which could cause equipment necessary for response to an accident to be unavailable on demand. Human error in these pre-initiator actions were incorporated into the systems analysis (fault trees) as a specific cause for system unavailability. As indicated above, both misalignment (restoration errors) and miscalibration were considered. Pre-initiator actions to be quantified were identified and selected from operating procedures and functional test procedures during the development of the system models and failure sequences. Qualitative evaluation removed certain errors from consideration. For example, calibration errors were omitted if the instrument limit (therefore the limit of miscalibration) was within technical specification limits. No numerical pre-screening was employed in the pre-initiator analysis. Human error probabilities (HEPs) were derived for ninety-nine errors surviving the qualitative screening. Quantification followed fairly closely the guidance provided in the ASEP HRA procedure. Plant-specific performance shaping factors and dependencies were treated in the quantification, and HRA modeling assumptions were, in general, verified by walkdowns, document review and discussion with plant personnel. The numerical values for the pre-initiator HEPs are generally consistent with the range of results in other PRAs. One pre-initiator action was identified as one of most important human errors in the IPE model -- common cause failure to restore reactor pressure instruments/switches that signal the permissive for core spray and low pressure coolant injection systems. This failure could prevent injection from both of these ECCS sources. Overall, the CNS pre-initiator analysis was one of the more thorough and better documented assessments of pre-initiator actions of the IPEs we have reviewed to date.

E.3.2 Post-Initiator Human Actions.

As indicated above, the HRA addressed both response-type and recovery-type actions. Actions to be included were identified from review of procedures and by discussion and interview with operations staff. IPE team members included individuals with plant operational experience. The actions identified and quantified are generally consistent with those analyzed in other BWR PRAs. A screening value of 0.5 for all post-initiator HEPs was applied in the initial quantification with a cutset truncation value of 1.0E-08/yr to eliminate actions/sequences that do not have a major impact on core damage frequency. Those response-type actions that were not screened out were quantified using the Daugherty and Fragola methodology described in Reference 2. The primary performance shaping factor considered was the timing of operator response (required vs. available time). Availability of procedures and "burden" (multiple or conflicting demands) on the operators were also considered. Dependencies among multiple actions in a sequence, and sequence-specific

influences on HEP values, particularly effects of timing, were treated. In the CNS analysis, post-initiator human actions were treated as diagnostic tasks only. The "execution" part of the human action is not treated. Typically the diagnosis portion of post-initiator human actions does dominate the execution part. However, most HRA techniques (including the Daugherty and Fragola approach) treat both parts. We consider this failure to treat the execution part of post-initiator human actions as a weakness of the CNS HRA approach, but do not consider it likely that it significantly alters the basic results or conclusions from the HRA or IPE.

Recovery actions were identified after initial quantification of the IPE and applied to sequences that survived the screening. "General" recovery actions, such as recovery of offsite power, were applied first. They were included in the model at the sequence level. A second truncation at $1.0E-08/\text{yr}$ was performed. General recovery actions are non-proceduralized. They were quantified primarily on the basis of analyst judgment, or from data-based models (e.g., for recovery of offsite power). "Specific" recovery actions were applied to cutsets still remaining above the $1.0E-08/\text{yr}$ truncation value. Specific recovery actions are proceduralized. They were quantified using the same methodology that was used for response-type actions; indeed some specific recovery actions are typical of response-type actions in other PRAs. Dependencies among multiple recovery actions in a sequence or cutset were addressed, and the HEPs were adjusted to account for dependencies. This iterative process of applying credit for recovery actions resulted in substantial reduction of the CDF. The submittal lists forty-three sequences that were screened out due to credit taken for recovery actions and indicates that several orders of magnitude reduction in estimated CDF resulted from credit taken for general and specific recovery actions. NUREG-1335 guidance emphasizes the importance of assuring that credit for recovery actions, in particular non-proceduralized recovery actions, is thoroughly justified. In our view, the information provided by the licensee in the submittal and responses to the NRC RAI is somewhat general and does not provide the thorough justification requested in NUREG-1335. This is a weakness in the IPE submittal documentation. It may or may not be a weakness in the IPE. That is, the credit taken for non-proceduralized recovery actions may or may not be appropriate and justified by plant-specific assessment. Based on our document-only review, we cannot conclude that credit is or is not justified.

E.4 Generic Issues and CPI

The licensee's consideration of generic safety issues (GSIs) and unresolved safety issues (USIs) and of containment performance improvements (CPI) recommendations are the subject of the front-end review, and back-end review, respectively. The licensee addressed decay heat removal to a limited extent. This issue is discussed by the front-end reviewer. Operator failure to depressurize the reactor is noted by the licensee as a significant contributor to risk for sequences involving loss of decay heat removal. A CPI related issue discussed by the back-end reviewer is the addition of a hardened vent. CNS plans to install (but did not credit in the IPE) a hardened vent system designed so that a torus purge line directs flow to the hardened vent system, which contains an air-operated isolation valve and a rupture disk. The current 2-inch vent line, which was assessed in the IPE and which is operable only if the

Standby Gas Treatment System is operable, was determined by the licensee to have little impact on accident mitigation and to be possibly detrimental with regard to radionuclide release. Venting, either in the current design or the future design, will require manual operator action performed by procedure.

E.5 Vulnerabilities and Plant Improvements

The submittal did not contain a specific definition of "vulnerability", nor did it contain a description of a systematic process or criteria for identifying vulnerabilities. There were insights derived from the IPE, and potential risk reducing enhancements were identified for further assessment. Reported insights from the front-end (Level 1) and back-end (Level 2) analyses included some related to human performance. The primary human-performance-related enhancement identified by the licensee as having been implemented is the EOP upgrade to Rev. 4 of the BWR Owners Group EPGs. Other procedure enhancements under consideration include improvements to:

- Procedure outlining improved battery loading schemes associated with a load study demonstrating potential extended battery life
- Procedure for bypassing the AC solenoid on the nitrogen supply line to the plant safety relief valves to reduce risk due to loss of pneumatic supply to SRVs
- Procedure associated with equipment modifications to provide a backup for service water pumps.

E.6 Observations

The following observations from our document-only review are pertinent to NRC's determination of whether the licensee's submittal meets the intent of Generic Letter 88-20:

- (1) The submittal and supporting documentation indicates that utility personnel were involved in the HRA, and that the walkdowns and documentation reviews constituted a viable process for confirming that the HFA portions of the IPE represent the as-built, as-operated plant (at least for the post-initiator error evaluation).
- (2) The licensee performed an in-house peer review that provides some assurance that the HRA techniques have been correctly applied and that documentation is accurate.
- (3) The analysis of pre-initiator human actions followed very closely a well documented, though simplified, HRA technique (ASEP). The analysis was relatively thorough and was well documented in comparison to other IPEs reviewed to date, and is considered a strength of the HRA. Both restoration errors and miscalibration were included. The processes for identification and selection of actions, qualitative screening (no numerical screening was performed), and quantification of pre-initiator actions was

reasonably comprehensive. The quantification involved some plant-specific assessment of performance shaping factors and dependencies influencing the probability of failure. Numerical results (human error probabilities) are generally consistent with values in other PRAs. One pre-initiator human action was identified as an important contributor to core damage frequency.

- (4) The treatment of post-initiator human actions was reasonably complete in scope. Both response-type and recovery-type actions were included. The processes for identification and selection of actions involved review of procedures and discussion with plant personnel. The numerical screening approach used values for human error probability and truncation frequency that appear to be appropriate for screening out unimportant actions/sequences without eliminating important contributors to CDF. The quantification process addressed some plant-specific performance shaping factors and sequence-specific influences, and addressed dependencies among multiple human actions.
- (5) A weakness in the treatment of post-initiator human actions is the failure to treat the execution part of the action. As discussed above, it is not possible to determine the overall significance of this weakness from our document-only review, but we do not expect that the basic results and conclusions of the HRA or IPE would be significantly modified if execution actions were treated.
- (6) A weakness in the submittal documentation is the discussion of the quantification of recovery actions, in particular the limited justification for credit taken for non-proceduralized recovery actions. Another weakness in documentation is the lack of discussion of quantification of human actions credited in the Level 2 analysis. These weaknesses in documentation may or may not represent weaknesses in the analysis.
- (7) The submittal did not provide a concise definition of vulnerability. No vulnerabilities were identified by the licensee. However, the licensee did identify insights from the Level 1 and Level 2 analyses relating to human-performance-related enhancements that have been made or will be considered for implementation by the licensee.

1. INTRODUCTION

This Technical Evaluation Report (TER) is a summary of the documentation-only review of the human reliability analysis (HRA) presented as part of the Nebraska Public Power District submittal of the Cooper Nuclear Station (CNS) Individual Plant Examination (IPE) to the U.S. Nuclear Regulatory Commission (NRC). The review was performed to assist NRC staff in their evaluation of the IPE and conclusions regarding whether the submittal meets the intent of Generic Letter 88-20.

1.1 HRA Review Process

The HRA review was a "document-only" process which consisted of essentially four steps:

- (1) Comprehensive review of the IPE submittal focusing on all information pertinent to HRA.
- (2) Preparation of a draft TER summarizing preliminary findings and conclusions, noting specific issues for which additional information was required from the licensee, and formulating requests to the licensee for the necessary additional information.
- (3) Review of preliminary findings, conclusions and proposed requests for additional information (RAIs) with NRC staff and with "front-end" and "back-end" reviewers.
- (4) Review of licensee responses to the NRC requests for additional information, and preparation of this final TER modifying the draft to incorporate results of the additional information provided by the licensee.

Findings and conclusions are limited to those that could be supported by the document-only review. No visit to the site was conducted. No discussions were held with plant personnel or IPE/HRA analysts, either during the initial review of the submittal, nor after receipt of licensee responses to NRC RAIs. No review of detailed "Tier 2" information was performed, except for selected details provided by the licensee in direct response to NRC RAIs. In general it was not possible, and it was not the intent of the review, to reproduce results or verify in detail the licensee's HRA quantification process.

1.2 Plant Characterization

CNS is a single-unit General Electric (GE) boiling water reactor (BWR-4) plant, with a Mark I containment. The unit is rated at 2381 MWt and 778 MWe (net). Commercial operation began in 1974. Similar units in operation are Brunswick and Hatch. Distinctive design features cited by the front-end reviewer include several, such as service water cross tie capability and fan coolers in the diesel generator ventilation system, which have associated human performance implications. A significant design feature cited by the front-end reviewer

which tends to decrease core damage frequency and has associated operator action is the ability to use the control rod drive (CRD) pumps for shutdown cooling. Two CRD pumps provides sufficient injection capability for core cooling during shutdown if all other cooling systems are lost. A significant human performance impact cited by the licensee is the upgrade of Emergency Operating Procedures (EOPs) to be consistent with Rev. 4 of the BWR Owners Group EPGs. The submittal notes in particular two risk-significant improvements associated with the upgraded procedures: (1) improvements in the directions to switch the Emergency Core Cooling System (ECCS) pumps to the emergency condensate storage tanks, and (2) procedures for venting. Operator failure to depressurize, either by incorrectly inhibiting the automatic depressurization system (ADS), or failure in manual depressurization using the safety relief valves (SRVs) was identified by the licensee as a significant contributor to core damage frequency (CDF) for CNS.

2. TECHNICAL REVIEW

2.1 Licensee IPE Process

2.1.1 Completeness and Methodology.

The HRA process addressed both pre-initiator actions (performed during maintenance, test, surveillance, etc.) and post-initiator actions (performed as part of the response to an accident). Pre-initiator actions considered included both restoration errors and miscalibration. Post-initiator actions included both response-type and recovery-type actions. The primary HRA techniques employed to quantify human error included the Accident Sequence Evaluation Program (ASEP) HRA procedure (Ref. 1) for pre-initiator actions, and the time reliability correlation (TRC) approach of Daugherty and Fragola (Ref. 2) for post-initiator actions. Plant-specific performance shaping factors and dependencies were considered to some degree in both pre-initiator and post-initiator analyses. Human errors were identified as significant contributors in accident sequences leading to core damage, and human-performance-related enhancements were identified and credited in the IPE/HRA or cited for future consideration. Licensee staff with knowledge of plant design, operations and maintenance had significant involvement in the HRA process. Procedures reviews, interviews with operations staff, and plant walkdowns helped assure that the IPE represented the as-built, as-operated plant. An independent review of the HRA performed by an independent contractor and in-house staff helped to assure appropriate use of HRA techniques.

2.1.2 Multi-Unit Effects and As-Built, As-Operated Status

CNS is a single-unit plant. The issue of multi-unit effects is not applicable.

The submittal notes (e.g., page 1-11) that the freeze date for the IPE was December 31, 1989 and that the IPE does not represent the current status of the plant. This is cited as the reason for not implementing at this time modifications based on insights gained from the IPE. The licensee states that insights gained and proposed modifications will be "revisited" after the IPE model is upgraded to reflect revisions to plant systems/operations since the cutoff date.

With regard to assuring that the IPE represented the plant as of the cutoff date, the submittal (Section 2.4.3) cites three walkdowns as the means by which the information used in the IPE was plant-specific and represented the as-built plant. The first was a containment walkdown which documented and familiarized consulting staff with CNS-specific containment features which could influence postulated severe accident progression. The second was conducted to support development of the system notebooks. While the submittal did not cite any HRA-specific issues or results from these walkdowns, the listing of typical types of information collected, especially in the second walkdown, suggest that HRA-specific information was obtained. For example, the walkdowns documented components that are not readily accessible because of height or radiation area and noted which MOVs have hand

wheels and which are locked in position. The third walkdown was conducted for the flooding analysis. No information on that walkdown specific to the HRA was noted in the submittal.

Additional evidence of verification of as-operated plant is provided by the discussions in Section 3.3.3.2.1 of the submittal which review three areas of operational practice that influence the pre-accident HEPs - procedures, man-machine interface, and training and qualifications. The writeup on procedures, in particular, suggests a significant effort to verify that assumptions made about operational practice in the HRA are indeed current practice. Specific operating, maintenance, test and calibration procedures, surveillance requirements, and other operational practices such as written checkoffs are cited that relate directly to HRA assumptions.

Overall, the submittal documentation indicates that the licensee took steps to provide reasonable assurance that the HRA-related aspects of the IPE model represented the as-built, as-operated plant at the time of the cutoff date of December 31, 1989. The submittal notes that there are modifications that have been made since the cutoff date that potentially have significant impact on the IPE results. In particular, and of special interest to the HRA review, the licensee expects that the EOP upgrade to Rev. 4 of the EPGs will provide significant risk reduction.

2.1.3 Licensee Participation and Peer Review.

The licensee's stated philosophy for staffing the IPE effort was to have a dedicated in-house PRA team trained and guided by a consultant experienced in nuclear plant PRAs. In the HRA area, the submittal notes that an experienced individual was not available in-house and had to be trained. Expertise and training in HRA was provided by Science Applications International Corporation (SAIC), the licensee's prime contractor for both the Level 1 and Level 2 PRA. The licensee staff member trained to be the licensee's "knowledgeable individual" in HRA was an experienced Engineering Technician with an Associates Degree with knowledge of CNS systems, layout, and documentation.

The Level 1 and Level 2 portions of the IPE were reviewed by both licensee personnel independent to the IPE project and by an independent consultant (ERIN, Inc.) As indicated above, no in-house expertise in HRA existed. However, substantial operating and systems knowledge was represented on the internal review team. The team included individuals from the Operations Support Group, Systems Engineers, the Instrument & Controls Group, the Nuclear Engineering Department, and the Nuclear Fuels Department. The Operations Support Group, Systems Engineers, and I&C Group are stationed at the Cooper site. The Operations Support Group includes licensed operators who develop and maintain EOPs. The ERIN team included experienced PRA analysts. HRA was listed as one of the areas of expertise included in the team. No results from the review were identified in the submittal. The submittal states (Page 5-3) that "The IPE comments and their resolutions were extensive and well documented. All of the comments were resolved to the satisfaction of the reviewers."

2.2 Pre-Initiator Human Actions

Errors in performance of pre-initiator human actions (i.e., actions performed during maintenance, testing, etc.) may cause components, trains, or entire systems to be unavailable on demand during an accident, and thus may significantly impact plant risk. Our review of the HRA portion of the IPE examines the licensee's HRA process to determine what consideration was given to pre-initiator human actions, how potential actions were identified, the effectiveness of quantitative and/or qualitative screening process(es) employed, and the processes for accounting for plant-specific performance shaping factors, recovery factors, and dependencies among multiple actions.

2.2.1 Pre-Initiator Human Actions Considered.

The CNS HRA addressed pre-initiator errors in maintenance, test and surveillance actions (the licensee refers to them as "pre-accident" errors) by incorporating human error into the systems analysis (fault trees) as a specific cause for system unavailability. Both misalignment (restoration errors) and miscalibration were considered.

2.2.2 Process for Identification and Selection of Pre-Initiator Human Actions.

The key concerns of our review regarding the process for identification and selection of pre-initiator human actions are: (a) whether maintenance, test and calibration procedures for the systems and components modeled were reviewed by the systems analyst(s), and (b) whether discussions were held with appropriate plant personnel (e.g., maintenance, training, operations) on the interpretation and implementation of the plant's test, maintenance and calibration procedures to identify and understand the specific actions and the specific components manipulated when performing the maintenance, test, or calibration tasks.

The submittal description of the systems analysis suggests a reasonable process was in place to identify pre-initiator human errors that could affect availability of equipment required to cope with abnormal events. The submittal notes that an experienced SRO with greater than 5 years experience participated directly in the pre-initiator HRA, provided walk-throughs of plant areas and control room, and acted as a liaison with other plant groups such as Maintenance, I&C, and Training. In addition, the submittal notes that the pre-initiator HRA work package was reviewed in detail by relevant plant departments to insure accuracy. Finally, the submittal (Section 3.3.3.2.1.1) provides a concise summary of the procedures and key procedure steps that were considered in the pre-initiator HRA. These include:

- Top level Conduct of Operations procedures for preparation, review and approval of all maintenance, calibration, surveillance, normal operating and administrative procedures

- Administrative controls over maintenance and test activities and over the surveillance program
- Guidance for evaluating the operability of components
- Requirements for the calibration program and calibration procedures
- General station and system operating procedures
- Specific maintenance, calibration, surveillance and I&C procedures.

The summary information presented in the submittal suggests that important factors influencing the probability of human error in pre-initiator actions were assessed and verified by examination of procedures. For example, requirements for written check-off or data recordings and signoff by the supervisor for Station Technicians performing daily or shift walk-round checks were verified, and specific procedures were cited in the submittal. Requirements for post-maintenance operability testing and surveillance sign-off sheets were verified, and specific cases were cited in the submittal. The overall impression from our review of the submittal is that a reasonably systematic and thorough assessment was made of potential pre-initiator human errors, and that significant errors were identified.

2.2.3 Screening Process for Pre-Initiator Human Actions.

No numerical screening was performed for pre-initiator human actions. Some potential restoration errors were excluded from the HRA on the basis that they were included in the estimated failure rate for equipment. The assumption was made that during regular testing of standby components or switching of operating components, failures to restore equipment would be identified in the plant-specific component failure database. If standby components were tested monthly, or operating components switched monthly, then it was assumed that the operating history was sufficient to have included human error into the component failure database, and that error was not assessed directly in the HRA. For all other restoration errors, an HEP was calculated and included in the appropriate fault tree(s). Miscalibration of an instrument was not analyzed if the instrument limit was within the technical specification limit.

2.2.4 Quantification of Pre-Initiator Human Actions.

The quantification of pre-initiator human errors followed fairly closely the guidance provided in the ASEP documentation (Ref. 1). An exception noted in the submittal is the assumption that a high degree of dependence exists between failures in miscalibration or restoration after calibration of certain level and pressure sensors that are physically and temporally separated, but would occur within one shift. This leads to a higher (more conservative) HEP than would be assigned by ASEP, which would assume zero dependence for these cases.

For restoration errors, the CNS analysis used the ASEP-recommended basic human error probability (BHEP) of 0.03, which is intended to represent a combination of a probability of 0.01 of an error of commission and 0.02 of an error of omission. For instrument miscalibration, the BHEP was assumed to consist of an error of commission only, representing improper calibration. The error of omission was assumed to be negligible, because it would involve two independent human errors (the omission error plus the previous miscalibration). Assumptions about dependencies were as follows:

- For failure to restore components, multiple pre-initiator errors of commission were assumed to have zero dependence
- Complete dependence was assumed for miscalibration of multiple instruments of the same type in the same location
- High dependence was assumed for miscalibration of multiple instruments of the same type in different locations.

As indicated earlier, it appears that assumptions made about operational practice related to maintenance, test and calibration were verified by examination of procedures and by discussions with appropriate maintenance, I&C and operations staff. Additional plant-specific factors considered were man-machine interface and training and qualifications. The submittal states (page 3-674) that, "The HRA approach assumes that tasks are performed by licensed qualified plant personnel who have functioned in their present position for at least six months. It also assumes that the environment in the control room is not adverse and that the levels of illumination and sound and the provision for physical comfort are adequate." The submittal indicates that plant areas where typical instrument calibration and other surveillance work is performed were assessed to verify that they are well illuminated and provide adequate space to perform the work. Components involved in maintenance, surveillance or other similar activities are labeled with both the component identification and functional description. Assumptions about minimum experience were verified by examining requirements in CNS procedures for personnel selection and training.

One pre-initiator action was identified as among the top ten most important human actions (as determined by the Fussel-Vesely importance ranking). That action, designated NBI-XHE-CF-PS52, is "Common Cause Failure to Restore PS52A2 and PIS52B or PS52C2 and PIS52D." These reactor pressure instruments/switches signal the valve opening permissive for core spray and LPCI at 400 psig. The valves cannot be opened with reactor pressure greater than 400 psig. Failure to properly restore these switches after maintenance/test can prevent injection from two ECCS sources.

In summary, the licensee's approach to quantification of pre-initiator human errors followed fairly closely the guidance for the ASEP pre-initiator HRA procedure provided in Reference 1. Adjustments were made to the generic BHEP based on plant-specific

consideration of important performance shaping factors. Plant-specific recovery factors were identified, and credit taken for them was appropriately justified. Dependencies were accounted for in a relatively simplified manner as prescribed for the ASEP procedure.

2.3 Post-Initiator Human Actions

Human errors in responding to an accident initiator, e.g., by not recognizing and diagnosing the situation properly, or failure to perform required activities as directed by procedures, can have a significant effect on plant risk. These errors are referred to as post-initiator human errors. (The CNS submittal refers to them as "post-accident" errors.) Our review assesses the types of post-initiator errors considered by the licensee, and evaluates the processes used to identify and select, screen, and quantify post-initiator errors, including issues such as the means for evaluating timing, dependency among human actions, and other plant-specific performance shaping factors.

2.3.1 Types of Post-Initiator Human Actions Considered.

There are two important types of post-initiator actions considered in most nuclear plant PRAs: (1) response actions, which are performed in response to the first level directives of the emergency operating procedures/instructions (EOPs, or EOIs); and, (2) recovery actions, which are performed to recover a specific failure or fault, e.g., recovery of offsite power or recovery of a front-line safety system that was unavailable on demand earlier in the event.

The CNS submittal does not present a clear categorization of types of post-initiator human actions examined, particularly with regard to defining "recovery" actions. The licensee's response to an NRC RAI provides some further description and some clarification. Though there still exists some ambiguity and minor inconsistencies in the definitions, we believe we have a reasonably clear understanding of the different types of human actions treated and how they were treated in the IPE modeling. It appears that both response-type and recovery-type actions, as we define them above, were treated. As we now understand the information in the submittal and the licensee's response to the RAI, the following process was used to address the different types of actions:

- 1) Some response-type actions were identified and included in the initial quantification (fault trees and event trees) using a screening value of 0.5 and a cutset truncation level of $1.0E-08/\text{yr}$.
- 2) Subsequently, recovery actions of two types were applied to sequences/cutsets with cutsets remaining above the $1.0E-08/\text{yr}$ level:
 - a) *General* recovery actions were applied at the sequence level. General recovery actions are non-proceduralized actions that involve recovery of systems/components associated with critical functions (our term). For example,

recovery of offsite power and recovery of power conversion system (PCS) are general recovery actions. Such actions would be classified as recovery actions in our definition above, and in most PRAs.

- b) Cutsets still remaining above the $1.0E-08/\text{yr}$ level were reviewed again for potential *specific* recovery actions. The definition of specific recovery action provided by the licensee is still somewhat ambiguous, but a major distinction from general recoveries is that the specific recoveries are proceduralized, typically in the EOPs, EOP Support procedures, or Abnormal Procedures. Some, e.g., "initiate RHR for suppression pool cooling or shutdown cooling," are typical of response actions in other PRAs. Others, e.g., "align service water cross-tie to reactor equipment cooling," are typical of recovery actions in other PRAs. Specific recoveries apparently were incorporated at the cutset level, which is typical and appropriate for recovery actions as defined in most PRAs. In general, specific recovery actions were quantified using the Daugherty and Fragola approach discussed in Section 2.3.4 below, whereas general recovery actions were quantified using data and/or subjective evaluation, based primarily on the time available vs. time required.

2.3.2 Process for Identification and Selection of Post-Initiator Human Actions.

The primary thrust of our review related to this question is to assure that the process used by the licensee to identify and select post-initiator actions is systematic and thorough enough to provide reasonable assurance that important actions were not inappropriately precluded from examination. Key issues are whether: (1) the process included review of plant procedures (e.g., emergency/abnormal operating procedures or system instructions) associated with the accident sequences delineated and the systems modeled; and, (2) discussions were held with appropriate plant personnel (e.g., operators or training staff) on the interpretation and implementation of plant procedures to identify and understand the specific actions and the specific components manipulated when responding to the accident sequences modeled.

The submittal does not discuss a "formal", systematic approach used to assure completeness in identifying all important post-accident human errors. However, there is ample evidence throughout the submittal discussions on accident sequence delineation that operator actions were identified as an integral part of the sequence and systems analysis, which involved review of procedures and discussion with operations staff. For example, significant operator actions are noted in virtually every sequence description. A comparison with other BWR PRAs indicated that the CNS study included the important post-initiator operator actions usually addressed for BWRs.

2.3.3 Screening Process for Post-Initiator Response Actions.

The submittal does not discuss pre-screening of post-initiator actions. The licensee's response to an NRC RAI indicated that an initial quantification was performed with a screening value of 0.5 for all human actions and a cutset truncation level of 1.0E-08/yr. This screening value of 0.5 is typical of screening values used in other PRAs. The combination of this screening value and cutset truncation level should screen out unimportant actions/sequences without eliminating important contributors.

2.3.4 Quantification of Post-Initiator Human Actions.

The quantification of post-accident human errors follows generally the approach outlined in the text by Daugherty and Fragola (Ref. 2), which in turn applies concepts of the Operator Action Tree (OAT) method reported in NUREG/CR-3010 (Ref. 3), along with concepts and techniques from a number of other sources. The Daugherty and Fragola approach uses time reliability correlations (TRCs) to obtain estimates of the probability of correct response (or the complementary probability of error) as a function of time available for the operator to respond. The submittal states that there are three primary factors that were considered in estimating the error probability:

- 1) Time available
- 2) Availability of relevant procedures
- 3) Degree to which operators become burdened by multiple tasks or conflicting demands.

The discussion in the submittal that describes how these factors were evaluated to obtain nominal HEPs appears to be a "generic" description of the Daugherty and Fragola methodology. In their response to the NRC RAI, the licensee stated that the CNS approach differed from the Daugherty and Fragola approach in two ways:

- 1) In the CNS approach, performance shaping factors other than timing and availability of procedures (rule-based actions) are incorporated into the burden factor and not treated directly, and
- 2) Post-accident tasks are evaluated principally as diagnosis tasks, and the "execution" phase is not treated.

This first difference may result in a somewhat more "generic" assessment of the impact of some of the performance shaping factors. However, the time reliability correlations in general are somewhat limited in their ability to easily accommodate plant-specific assessment of performance shaping factors other than time. They are based on simulator data available from published studies, and usually have limited capacity to adjust the

correlation for individual plant-specific factors. This difference from the Daugherty and Fragola approach does not appear to be important.

The second difference, treating only the diagnostic part of the post-initiator actions, is inconsistent with most HRA techniques and with most HRAs reviewed to date. It is generally true that the diagnostic portion of post-initiator actions is the more important contributor to risk. Typically, an error in diagnosis is less likely to be immediately recognized and recovered, and the consequences of error are more significant. However, this certainly is not true in all cases. Most HRA techniques, and most analyses reviewed to date, have considered both the diagnostic (cognitive) portion and the execution (action) portion of post-initiator actions. (We recognize that the distinction between "cognitive" and "action" phases is not as distinct as it is assumed in most of the HRA techniques and that diagnosis and action are a dynamic interactive process. However, the general distinction is valid and is useful for simple models of human response.) While we consider this assumption a weakness of the post-initiator HRA (in comparison to other IPEs) it is not possible from our document-only review to determine the quantitative impact of the assumption on the CNS results. As indicated above, we would expect that in general the diagnosis portion dominates the risk contribution. Accounting for failure in the execution phase would increase the probability of failure for post-initiator human actions, but probably would not substantially impact the basic results and conclusions from the HRA and the IPE.

To implement the Daugherty and Fragola approach, nominal HEP values are selected from data tables which represent the time reliability correlations. The TRCs are based primarily on results from reported simulator studies. The selection is based on assumptions made about each of the three factors above - timing, availability of procedures, and burden. The time available for diagnosis T_A , is calculated as:

$$T_A = T_1 - (T_2 + T_3)$$

where:

- T_1 = The maximum amount of time available during which, if the necessary human actions are completed, subsequent core damage is prevented
- T_2 = Time from the occurrence of an abnormal event to the annunciation of the event; i.e., when the operator is alerted that the failure (or symptom) has occurred
- T_3 = The minimum time required to implement the actions in response to the diagnostic judgments and have the necessary system(s) act to prevent core damage (usually, just the time required to take the operator action).

The submittal discusses and presents sample blank tables of the input data that were assessed to quantify the HEPs for post-accident errors. These sample tables and the general type of information contained in each are summarized in Table 2-1 below.

2.3.4.1 Consideration of Timing. Several techniques for establishing the estimated times are described in general, but it is difficult to find specific statements in the submittal defining precisely what sources or techniques were actually used for the CNS. The licensee's response to an NRC RAI clarified the approaches used for CNS. It also included samples of the structured forms used to guide and record the estimation of time. T_1 was calculated from plant-specific analysis using an accident code such as MAAP and from discussion with operators; and, if such analyses did not exist, relevant analysis from the NUREG-1150 Peach Bottom study were used. The licensee states that estimates of the required time for operators to complete the action were obtained "verbally from SROs or from Job Performance Measures," and that all operator action times obtained from SROs were then doubled. The required time T_3 was the sum of the travel time (significant for out-of-control-room actions) and the actual manipulation time. Travel times were estimated by operators for conditions representative of the accident situation, taking into account impacts of temperature, radiation levels, and accessibility. Estimates of manipulation time were increased if it was judged that complexity or difficulty of the task was more than nominal. While direct measurement of typical times, e.g., in the simulator or in time walkdowns, is the preferred approach for estimation of times, operator judgment has been used in other accepted PRAs, and is considered a reasonable source, particularly when operator estimates are doubled as was done in the CNS analysis.

2.3.4.2 Other Performance Shaping Factors Considered. The submittal states (page 3-675) that, having estimated times, the next factor to consider is whether the operators' response will be "rule-based" or "recovery actions". The assumption is that the tables of HEP values have accounted for the differences in these two types of responses. The submittal states that all EOP-directed actions are considered "rule-based".

The third major factor said to be considered is operator "burden". In Reference 2, the concept of burden is fairly broad and includes, in addition to time stress, "diagnostic burden", "decision making burden", "command and control burden", and "physiological burden". Based on the submittal discussion, it appears that consideration is limited to the number of abnormal events being dealt with simultaneously. Each accident sequence consists of numerous cutsets. The cutsets are reviewed to identify specific failures. Cutsets that result in essentially the same accident conditions and lead the operators to the same procedures are grouped together. In some cases, operators may have to respond to different specific events within the response to the overall accident event, and may have to use different procedures. If there is more than one abnormal event in approximately

Table 2-1 Input Data for Post-Initiator Human Actions

| <u>TABLE</u> | <u>KEY INFORMATION</u> |
|--------------|---|
| 3.3.3.3-A-1 | Accident Sequence Description - event tree, sequence number, sequence designator, sequence description, accident type, accident conditions, applicable procedures |
| 3.3.3.3-A-2 | Sequence and Cutset Timing - event/occurrence of most interest, time (T_2) for the operator to become alerted, annunciator/indication |
| 3.3.3.3-A-3 | Cutset Failure and Potential Operator Action - identifies specific actions required to cope with the abnormal event; includes a general event description, symptoms, specific abnormal events (each different procedure is considered a new abnormal event), possible actions, specific activities required to perform the actions and procedures |
| 3.3.3.3-A-4 | Sequence and Cutset Available Time - Documents the process and data to estimate the maximum time available to correctly diagnose an abnormal event and initiate action (T_A); includes maximum time available to prevent core damage (T_1), time operator is alerted (T_2), time required to take the necessary actions (T_3) |
| 3.3.3.3-A-5 | Operator Action Performance Time - location of the action, travel time, performance time, and total time required for the operator to initiate the actions necessary to prevent core damage (T_3) |
| 3.3.3.3-A-6 | Procedure Usage - documents information obtained about the procedure used, if any; includes procedure number, step number, and frequency of training on the procedure |
| 3.3.3.3-A-7 | HEP Analysis, One Abnormal Event, With Procedures - documents the HEP estimation for cases in which there is one abnormal event (distinct operator action with different procedures) within a cutset; includes the median HEP, mean HEP, and error factors, taken from the appropriate table based on the time estimated for T_A |
| 3.3.3.3-A-8 | HEP Analysis, One Abnormal Event, No Procedures |
| 3.3.3.3-A-9 | HEP Analysis, More Than One Abnormal Event, With Procedures |
| 3.3.3.3-A-10 | HEP Analysis, More Than One Abnormal Event, No Procedures |

the same time frame, the operator is considered burdened, and a different table of HEPs is used. An assumption made is that events separated by more than 15-20 minutes are treated as single events (operators not burdened). The licensee's response to the NRC RAI indicates that other performance shaping factors were incorporated into the burden factor, but details are not provided.

Once the assessment of the three primary factors - time, availability of procedures, and burden - was completed, the nominal HEP is obtained from one of the four tables based on the time reliability correlations and associated information in Reference 2. Each table corresponds to one of four combinations of two factors: one abnormal event, or more than one event; with or without procedures. This approach uses "generic" data, but permits some consideration of the three plant-specific factors as described above.

2.3.4.3 Quantification of Recovery Actions. The submittal did not clearly specify the approach for quantification of recovery actions. The licensee's response to an NRC RAI indicates (though does not precisely state) that general recovery actions were quantified either a) using data based models, e.g., for loss of offsite power, or b) by subjective judgment of the HRA analysts based largely on time available. The licensee states that time available was determined from "plant-specific thermal-hydraulic calculations and other available calculations, or engineering judgment," and that specific recovery actions were quantified using a more detailed analysis, which "generally consists of post-accident HRA analysis." We take this latter statement to mean that specific recovery actions were quantified using the Daugherty and Fragola methodology.

As noted earlier, the licensee's response indicates that general recovery actions typically apply to all cutsets in a given sequence and were incorporated into the IPE model at the sequence level. Specific recovery actions typically are cutset-dependent and were incorporated at the cutset level.

In response to the NRC RAI, the licensee provided a brief discussion of plant-specific evaluation of out-of-control room actions, using a specific example from the IPE model, CRD-XHE-FO-CRDEM, failure to maximize CRD flow to the reactor vessel. From this discussion it is apparent that the licensee considered plant-specific factors that influence human error probability. The diagnosis action, key indications, parallel tasks, environmental factors such as radiation and temperature, and timing were considered, at least qualitatively. The example discussion did not indicate how the performance shaping factors were quantified. It did suggest that these plant-specific factors were considered on a case-by-case basis for actions taken outside the control room.

NUREG-1335 guidance to the licensee (page C-19 of NUREG-1335) is that credit should not be taken for non-proceduralized recovery actions without proper justification. NUREG-1335 does not discuss further what constitutes "proper" justification, though it does indicate that available time alone is not sufficient justification. As indicated above, the general recovery actions were not proceduralized. The NRC RAI requested that the

licensee discuss plant-specific analysis conducted to verify that HEP values for non-proceduralized actions were realistic and credit for those actions is justified. The licensee's response indicated that once the failure is investigated and the failure mode identified, repair is performed per procedure and that the personnel doing the investigation are well trained. In our view, this discussion does not fully explain/justify the credit taken for non-proceduralized actions. The fact that the specific repair actions required "once the failure is investigated and the failure mode identified" are proceduralized is not the central issue. The issue is whether the identification and investigation of the failure is likely to be carried out successfully in the time available. The licensee's "justification" for crediting the non-proceduralized actions still seems primarily to be that time is available, which NUREG-1335 indicates is not sufficient justification. We do note that HEP values assigned to these actions are fairly high (0.1 or greater for times under about 2 hours). We also note that other PRAs have taken credit for some non-proceduralized actions. The credit taken in the CNS analysis may or may not be appropriate. And, there may or may not be more in-depth plant-specific assessment that supports the credit taken. Based on our review of the material available for review, we conclude that at least there is a weakness in the submittal documentation justifying the credit taken for these actions. This weakness in the documentation may or may not represent a weakness in the IPE analysis. Indeed, we would extend this specific comment on the justification of credit for non-proceduralized recovery actions to the documentation of the analysis of operator recovery actions overall. The discussion provided by the licensee of the quantification process for recovery actions lacks clarity and does not provide a high degree of confidence that credit for recovery actions is justified.

2.3.4.4 Consideration of Dependencies. An important concern in HRA is the determination of how the probability of success or failure on one human action may be related to success or failure on another. Human behavior typically is highly dependent on the context in which the performance takes place - success or failure on a preceding action, performance of other team members in parallel or related actions, assumptions about the expected level of performance of other team members based on past experience, and many other factors. The human error probability estimates for HRA are conditional probabilities. If dependencies are not specifically accounted for, and HEPs are treated as independent, the probabilistic combination of HEPs can lead to an unrealistically low estimate of human performance overall (i.e., of the joint human error probability), and to a significant underestimate of risk.

The submittal provided very little specific information regarding how dependencies were treated. The licensee's response to the NRC RAI provided some clarification. Dependencies among multiple human actions in fault trees or event trees were treated through the use of the burden factor. Multiple human actions are considered burdened, and the HEPs are more "conservative", i.e., higher. In addition, if evaluation of the human action involved combining two or more HEPs, only one was quantified at the "nominal" value, and the others were retained at the screening value of 0.5. This is essentially equivalent to using the THERP (Ref. 4) dependency modeling and assuming

high dependency. Sequence-specific impacts on human actions modeled as top events in event trees were accounted to some extent through the consideration of timing and through the burden factor. The estimated required time to perform the accident was assumed to be the same for all sequences. However, the time available (which is the predominant factor influencing the estimated HEP) was considered on a sequence-specific basis. If the action was considered burdened for any sequence, then it was considered burdened for all sequences, which probably is a "conservative" approach.

Dependencies among multiple recovery actions were assessed on a case-by-case basis when there were multiple recovery actions in a sequence. In most cases, the evaluation concluded that only one recovery action should be included per cutset. In other cases decisions about dependencies were made on the basis of analyst judgment. The licensee cites three examples (which they indicate were "allowed" in NUREG/CR-4550) in which two recovery actions were included in a cutset:

- 1) Failure to recovery offsite power and failure to recover onsite power
- 2) Failure to recover offsite power and failure to recovery an injection system, and
- 3) Failure to recover the PCS and failure to recover an injection system.

In case 1, the recovery probabilities were derived from a data-based model, and dependencies are included in the data. For the other two cases, it was determined by the licensee that the two actions could be treated as independent because there were different teams of personnel responsible for the actions. We cannot evaluate this assumption without more detailed information on the particular actions involved and the operational practice at CNS. The licensee states that if several combinations of recovery actions were possible, the combination resulting in the smallest nonrecovery probability was utilized.

Overall, these approaches for treating dependencies among multiple actions in fault trees and event trees and for modifying HEPs to account for sequence-specific performance shaping factors are somewhat simplified, but are generally consistent with the capabilities of the basic HRA methodology selected, and are generally reasonable in comparison to other approaches that have been used in other PRAs. In our view, credit for more than one recovery action per cutset should be considered very carefully. The dynamic nature of accident response, especially when recovery action is required beyond the "normal" response to a given accident initiator, can create a high degree of dependency among recovery actions. In the case of CNS, the licensee has clearly identified the importance of accounting for dependencies, has analyzed the actions case-by-case, and has either quantitatively adjusted the HEP values or has determined that adjustment is not necessary. While we may or may not have come to the same judgment given the detailed information available to the licensee, the *process* used by the licensee is reasonable.

2.3.4.5 Treatment of Operator Actions in the Internal Flooding Analysis. The CNS assessment of internal flooding consisted primarily of review of results of a previous study performed for NRC by Sandia National Laboratory supported by plant walkdowns of potential areas of flooding. We identified no discussion of credit taken for human actions, except a general statement (page 3-724) that no credit was taken for "heroic actions to restore decay heat removal equipment."

2.3.4.6 Sequences Screened Out Due to Credit for Recovery Actions. Section 3.4.1.1.6.1 of the submittal discusses sequences screened out due to credit taken for recovery actions. Table 3.4.1-5 of the submittal lists the top forty three sequences screened out due to credit for recovery actions. Original estimates (without recovery credit) range from a high of $9.90E-03$ down to $1.80E-05$. The table shows that in many cases, there are a number of specific recoveries credited for a particular accident sequence, and in some cases more than one general recovery is included. As discussed above, the licensee's response to the NRC RAI indicated that dependencies among multiple recovery actions were addressed, and in most cases there was only one recovery action per cutset. HEP values for specific recovery actions range from a high of $4.20E-02$ to a low of $2.1E-05$. Most of the values are in lower end of this range ($2.1E-05$ to $6.9E-04$). These values used for specific recovery actions are generally low in comparison to values typically used for recovery actions; but as indicated previously, include actions which are more typical of response-type actions in other PRAs. The general recovery actions, such as recovery of diesel generator hardware failure, are assigned higher (more conservative) HEPs typical of recovery actions in other PRAs. Collectively, the reduction in CDF due to credit for recovery actions is substantial. Table 3.4.1-5 shows that CDF is reduced several orders of magnitude due to credit for recovery actions, though it is not possible to tell from the submittal information how much is due to general (non-proceduralized) vs. specific (proceduralized) recoveries. As indicated earlier, the lack of clarity in the discussions of the treatment of recovery actions is considered a weakness of the IPE submittal documentation which may or may not represent a weakness in the analysis.

2.3.4.7 Treatment of Operator Actions in the Level 2 Analysis. A number of operator actions were included in the containment event trees (CETs) in the Level 2 analysis. Top events in the CETs that included human action were listed in the submittal (Table 4.6-2). Included are:

- AC power not restored early
- Late AC power is not restored when the event is a station blackout
- Alternate flow (core injection with condensate or service water) is not initiated
- Operator fails to depressurize after core damage
- Human error results in a failure to restore control rod drive (CRD) system flow to the vessel
- Operator fails to provide CRD flow to debris
- Operator fails to actuate sprays early to depressurize containment
- Operator fails to actuate sprays to cool debris

- Operator fails to vent containment early
- Operator fails to vent containment late.

We could not identify any discussion of the quantification approach for the operator actions included in the Level 2 analysis. The absence of this discussion is a weakness of the submittal documentation. It may or may not represent a weakness in the IPE analysis.

2.3.4.8 GSI/USI and CPI Recommendations. The licensee's consideration of generic safety issues (GSIs) and unresolved safety issues (USIs) and of containment performance improvements (CPI) recommendations are the subject of the front-end review, and back-end review, respectively. The licensee addressed decay heat removal to a limited extent. This issue is discussed by the front-end reviewer. Operator failure to depressurize the reactor is noted by the licensee as a significant contributor to risk for sequences involving loss of decay heat removal. A CPI related issue discussed by the back-end reviewer is the addition of a hardened vent. CNS plans to install (but did not credit in the IPE) a hardened vent system designed so that a torus purge line directs flow to the hardened vent system, which contains an air-operated isolation valve and a rupture disk. The current 2-inch vent line, which was assessed in the IPE and which is operable only if the Standby Gas Treatment System is operable, was determined by the licensee to have little impact on accident mitigation and to be possibly detrimental with regard to radionuclide release. Venting, either in the current design or the future design, will require manual operator action performed by procedure.

2.4 Vulnerabilities, Insights and Enhancements

2.4.1 Vulnerabilities.

The submittal did not contain a specific definition of "vulnerability", nor did it contain a description of a systematic process or criteria for identifying vulnerabilities. The licensee did identify insights derived from the IPE and noted potential risk reducing enhancements identified for further assessment. Insights from the Level 1 and Level 2 analyses that relate to human performance and potential human-related plant improvements identified in the submittal are summarized in the following section.

2.4.2 IPE Insights Related to Human Performance.

2.4.2.1 Insights from the Level 1 Analysis. The importance of human performance to estimated core damage frequency is discussed in the submittal. A listing of nine failures identified as dominant contributors to CDF includes one operator error - failure to depressurize (inhibiting ADS or manually using SRVs). Calculations of risk reduction worth show that this error is the fourth largest contributor to risk reduction worth. The pre-initiator human error "common cause miscalibration of NBI-PS-52 pressure switches" was identified as having the fourth highest risk achievement worth. Sensitivity studies performed as part of the Level 1 analysis included investigations of the impact of

human-related performance and potential enhancements. Examples of the sensitivity studies noted that have some relationship to human performance issues are:

- 1) The impact on core damage frequency if, for the Loss of Service Water initiator, the new EOPs (based on Rev. 4 of the BWROG EPGs) were not used. This was the exception noted earlier in which CNS did take credit for the new EOPs. The sensitivity study showed that the CDF would be raised from $7.97\text{E-}05/\text{yr}$ to $2.81\text{E-}04/\text{yr}$.¹
- 2) The use of alternate room cooling for ECCS pump rooms has been proceduralized since the IPE freeze date. Accounting for this recovery action (non-recovery probability of $3.0\text{E-}04$) lowered the core damage frequency slightly to $7.81\text{E-}05/\text{yr}$.
- 3) Plant data indicate there has been a drop in the initiator frequency for the T2 sequence. This drop is believed to be due to improvements in maintenance, training, and management practices. A sensitivity study using the revised estimated frequency reduced the CDF to $7.69\text{E-}05/\text{yr}$.
- 4) Due to the fact that the action had not been proceduralized or tested, no credit was taken in the IPE for the ability to cross-connect the Circulating Water Pumps and the Service water going to the Turbine Equipment Cooling (TEC) Heat Exchangers. With this cross-connect, the TEC system could operate without service water, and the plant would not lose PCS during loss of service water sequences. A non-recovery probability of $7.0\text{E-}04$ was estimated for failure to perform this recovery action when proceduralized and tested. The CDF was lowered to $7.11\text{E-}05/\text{yr}$.

Human error, in particular failure to manually depressurize, was noted as a significant contributor to potential problems in assuring decay heat removal. Other major equipment contributors to loss of decay heat removal have associated operator actions that were included in the HRA. These findings on decay heat removal and contributions from human performance are consistent with results of previously accepted PRAs.

¹ In communication between NRC and the licensee after the IPE was submitted the licensee indicated that the licensee's review of the accident sequences in conjunction with the Level 2 analysis indicated that one of the dominant core damage scenarios initiated by total loss of service water in fact does not likely lead to core damage as originally predicted in the Level 1 analysis. A sensitivity study showed that the elimination of the associated sequences reduces the CDF estimate to $7.10\text{E-}05/\text{yr}$. This TER continues to use the value of $7.97\text{E-}05/\text{yr}$ reported in the original submittal as the overall CDF estimate, since it is the referenced value at the time our review was performed.

2.4.2.2 Insights from the Level 2 Analysis. A significant human performance related insight from the Level 2 assessment was that the new EOPs allow for earlier initiation of containment spray, which adds water to the drywell and significantly decreases the probability of drywell liner melt-through, and thereby helps to mitigate some accident sequences in which the vessel is breached.

A sensitivity study for the Level 2 results addressed failure of operators to vent containment. The study concluded that venting with the current configuration (a 2-inch line and only if the Standby Gas Treatment System is operable), has little benefit for accident mitigation and may lead to earlier release of radionuclides that otherwise would have been retained in containment. In addition to venting, the back-end discussions identify the following issues with human performance related implications as important to radionuclide retention:

- Recovery of AC power (station blackout)
- Drywell vacuum breaker reclosure
- Human error in the actuation of injection and/or spray systems.

Three sensitivity studies were performed to assess the impact of non-recovery of AC power. The first assumed failure (probability 1.0) of early recovery; the second failure of both early and late recovery; and, the third, the optimistic case of assured early recovery (failure probability 0.0). Results demonstrate that AC recovery is critical to mitigation of accidents initiated by loss of station power. If early AC recovery is assured, the containment is not challenged; late recovery or failure to recover substantially increases the probability of vessel failure and core-concrete interaction.

The issues of drywell failure and vacuum breaker re-closure, which relate to suppression pool bypass, were said to be addressed by inspection; no sensitivity studies were performed. Neither were sensitivity studies were reported for human error in the actuation of injection and/or spray systems.

These insights identified by the licensee and the sensitivity studies on human-performance-related issues are an indication of the licensee's awareness of the contribution of human performance to plant risk and of the appropriate use of risk-based methods to identify the significance of actual and potential enhancements.

2.4.3 Human-Related Enhancements.

The primary human-related plant improvement identified in the IPE is the upgrade of the EOPs to Rev. 4 of the BWR Owners Group EPGs. While this upgrade was not a direct result of the IPE, insights obtained from the IPE suggest specific points of potential risk reduction anticipated from incorporation of the upgrade. Two items in

particular associated with the upgraded procedures were cited by the licensee as risk-significant: (1) improvements in directions to switch the ECCS pumps to the emergency condensate storage tanks, and (2) procedures for venting were cited as important improvements. New procedures already in place also include procedures for handling the Service Water initiated scenario and new guidance for alternate room cooling for the ECCS pump rooms. Credit was taken in the IPE for the new Service Water procedures, but not for any other procedure changes made since the cutoff date of December 31, 1989. As indicated earlier, the submittal states that no modifications currently are planned to address insights from the IPE, because the IPE models do not reflect such changes in plant status since the cutoff date. Potential improvements will be revisited after the IPE model is upgraded to reflect these changes.

Other human-related potential improvements that will be considered by the licensee (no commitments identified) are procedure improvements associated with equipment-related insights, including:

- Procedure outlining improved battery loading schemes associated with a load study demonstrating potential extended battery life
- Procedure for bypassing the AC solenoid on the nitrogen supply line to the plant safety relief valves to reduce risk due to loss of pneumatic supply to SRVs
- Procedure associated with equipment modifications to provide a backup for service water pumps.

3. CONTRACTOR OBSERVATIONS AND CONCLUSIONS

The purpose of our document-only review is to enhance the NRC staff's ability to determine with the licensee's IPE met the intent of Generic Letter 88-20. The Generic Letter had four specific objectives for the licensee:

- (1) Develop an appreciation of severe accident behavior.
- (2) Understand the most likely severe accident sequences that could occur at its plant.
- (3) Gain a more quantitative understanding of the overall probability of core damage and radioactive material releases.
- (4) If necessary, reduce the overall probability of core damage and radioactive material release by appropriate modifications to procedures and hardware that would prevent or mitigate severe accidents.

With specific regard to the HRA, these objectives might be restated as follows:

- (1) Develop an overall appreciation of human performance in severe accidents; how human actions can impact positively or negatively the course of severe accidents, and what factors influence human performance.
- (2) Identify and understand the operator actions important to the most likely accident sequences and the impact of operator action in those sequences; understand how human actions affect or help determine which sequences are important.
- (3) Gain a more quantitative understanding of the quantitative impact of human performance on the overall probability of core damage and radioactive material release.
- (4) Identify potential vulnerabilities and enhancements, and if necessary/appropriate, implement reasonable human-performance-related enhancements.

The following observations from our document-only review are pertinent to NRC's determination:

- (1) The submittal and supporting documentation indicates that utility personnel were involved in the HRA, and that the walkdowns and documentation reviews constituted a viable process for confirming that the HRA portions of the IPE represent the as-built, as-operated plant (at least for the post-initiator error evaluation).

- (2) The licensee performed an in-house peer review that provides some assurance that the HRA techniques have been correctly applied and that documentation is accurate.
- (3) The analysis of pre-initiator human actions followed very closely a well documented, though simplified, HRA technique (ASEP). The analysis was relatively thorough and was well documented in comparison to other IPEs reviewed to date, and is considered a strength of the HRA. Both restoration errors and miscalibration were included. The processes for identification and selection of actions, qualitative screening (no numerical screening was performed), and quantification of pre-initiator actions was reasonably comprehensive. The quantification involved plant-specific assessment of performance shaping factors and dependencies influencing the probability of failure. Numerical results (human error probabilities) are generally consistent with values in other PRAs. One pre-initiator human action was identified as an important contributor to core damage frequency.
- (4) The treatment of post-initiator human actions was reasonably complete in scope. Both response-type and recovery-type actions were included. The processes for identification and selection of actions involved review of procedures and discussion with plant personnel. The numerical screening approach used values for human error probability and truncation frequency that appear to be appropriate for screening out unimportant actions/sequences without eliminating important contributors to CDF. The quantification process addressed some plant-specific performance shaping factors and sequence-specific influences, and addressed dependencies among multiple human actions.
- (5) A weakness in the treatment of post-initiator human actions is the failure to treat the execution part of the action. As discussed above, it is not possible to determine the overall significance of this weakness from our document-only review, but we do not expect that the basic results and conclusions of the HRA or IPE would be significantly modified if execution actions were treated.
- (6) A weakness in the submittal documentation is the discussion of the quantification of recovery actions, in particular the limited justification for credit taken for recovery actions, in particular non-proceduralized recovery actions. Another weakness in documentation is the lack of discussion of quantification of human actions credited in the Level 2 analysis. These weaknesses in documentation may or may not represent weaknesses in the analysis.
- (7) The submittal did not provide a concise definition of vulnerability. No vulnerabilities were identified by the licensee. However, the licensee did identify insights from the Level 1 and Level 2 analyses relating to human-performance-related enhancements that have been made or will be considered for implementation by the licensee.

4. DATA SUMMARY SHEETS

Important Operator Actions/Errors:

The ten most important human errors (Fussel-Vesely criteria) are in order:

1. Operator inhibits ADS (fails to depressurize)
2. Non-recovery of offsite power
3. Operator fails to manually depressurize using SRVs
4. Non-recovery of diesel hardware failures
5. Non-recovery of service water from repair
6. Common cause failure to restore reactor pressure switches
7. Non-recovery of critical switchgear room ventilation within one hour
8. Non-recovery of diesel generator common cause failure
9. Non-recovery of diesel generator from maintenance
10. Failure to prevent rapid overfill with HPCI unavailable

Human-Performance Related Enhancements:

- Implemented human factor improvements or enhancements stemming from HRA:

The primary improvement is incorporation of the new EOPs. Other procedures improvements, sometimes related to equipment changes, have been implemented.

- Human factor improvements or enhancements under consideration:
 - Procedure outlining improved battery loading schemes associated with a load study demonstrating potential extended battery life
 - Procedure for bypassing the AC solenoid on the nitrogen supply line to the plant safety relief valves to reduce risk due to loss of pneumatic supply to SRVs
 - Procedure associated with equipment modifications to provide a backup for service water pumps.

REFERENCES

1. A.D. Swain, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," NUREG/CR-4772, February, 1987.
2. Daugherty, E.M., Jr. and J.R. Fragola, *Human Reliability Analysis, A Systems Approach with Nuclear Power Plant Applications*, John Wiley & Sons, New York, 1988.
3. Hall, R.E., et al., "Post-Event Human Decision Errors: Operator Action Tree/Time Reliability Correlations, NUREG/CR-3010, USNRC, November, 1982.
4. A.D. Swain and Guttman, H.E., "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report," NUREG/CR-1278F, USNRC, August, 1983.