MILLSTONE NUCLEAR POWER STATION, UNIT NO. 2

INDIVIDUAL PLANT EXAMINATION

TECHNICAL EVALUATION REPORT

(HUMAN RELIABILITY ANALYSIS)

Enclosure 4

CONCORD ASSOCIATES, INC.

Systems Performance Engineers

CA/TR-94-019-36

MILLSTONE NUCLEAR POWER STATION UNIT 2

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 Technology

Draft Report, November, 1994
Final Report, November, 1995

11915 Cheviot Dr.
Herndon, VA 22070
(703) 318-9262

725 Pellissippi Parkway
Knoxville, TN 37932
(615) 675-0930

6201 Picketts Lake Dr.
Acworth, GA 30101
(404) 917-0690

CA/TR-94-019-36

MILLSTONE NUCLEAR POWER STATION UNIT 2

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 Technology

Draft Report November, 1994
Final Report November, 1995

CONCORD ASSOCIATES, INC.
Systems Performance Engineers

725 Pellissippi Parkway
Knoxville, TN 37932

Contract No. NRC-04-91-069
Task Order No. 36

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont'd)

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 Millstone Nuclear Power Station Unit 2 Individual Plant Examination (IPE) submitted by Northeast Utilities (NU) 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

The Millstone Unit 2 plant is a Combustion Engineering (CE) pressurized water reactor (PWR) with a power rating of 2,700 MWt and 863 MWe. It is a two-loop plant, with each loop including a steam generator and two reactor coolant pumps. Initial operation was in December, 1975. Design features of particular significance with regard to operator action include:

- Automatic switchover of ECCS from injection to recirculation
- Ability for bleed-and-feed operation
- Fire water backup for Condensate Storage Tank (CST)

E.2 Licensee IPE Process

Utility personnel were involved in the HRA. All of the front-end analysis (including the HRA) and 80% of the back-end analysis were performed by utility staff. The submittal did not indicate that plant walkdowns were performed specifically for the IPE; but, the submittal does note that the utility has a strong "Living PRA" program which provides assurance that the IPE represents the as-built, as-operated plant. The licensee performed an in-house peer review of the IPE (including the HRA) to help assure that the PRA/HRA techniques were correctly applied. The HRA approach employed by the licensee considered both pre-initiator human actions (actions during maintenance, test, etc.) that could cause failure of important equipment on demand during an accident and post-initiator human actions (those taken in response to an accident event). However, the pre-initiator analysis was relatively limited, and quantitative assessment of human error focused primarily on post-initiator actions. The licensee identified and discussed important human actions. The licensee identified no vulnerabilities. No insights or enhancements related to human performance were identified.

E.3 Human Reliability Analysis

E.3.1 Pre-Initiator Human Actions

The licensee considered pre-initiator errors in maintenance, test and surveillance actions by incorporating human error into the systems analysis (fault trees) as a potential cause for system

unavailability. Both calibration errors and restoration errors were considered. However, based on the information available from the licensee, the analysis appears to have been relatively limited in breadth and depth. Quantification of calibration errors appears to have been limited to RWST Level Sensor Miscalibration. In fact, the specific error considered was actually a restoration error - failure to properly restore the sensing line valve after calibration. The potential for error in actual calibration was dismissed as unlikely by the licensee without specific analysis. Analysis of RWST Level Sensor miscalibration appears to have included review of procedures and plant experience (incident reports). Estimates of the human error probability (HEP) were stated by the licensee to have been calculated using the THERP methodology. Details of the THERP calculation are not provided. The HEP value calculated for the failure to open the root valve after miscalibration appears to be reasonable (i.e., typical of values for similar actions in other PRAs). Substantial credit was given for the likelihood of operator detection of the latent failure during required surveillance. It is not clear that this credit would be valid in the event that all four channels were miscalibrated due to a "common-cause" error. In general, we find the assessment of calibration errors to be limited in scope and depth. While it is not possible to determine whether or not this general weakness has a significant impact on the quantitative results of the IPE, the information provided by the licensee does not present a convincing argument that the impact of miscalibration is essentially insignificant.

The analysis of restoration errors appears to have been limited to valve misalignments, and probably to a single case of failure to reopen valves in the high pressure safety injection (HPSI) system following maintenance. The estimated HEP for that case was calculated using THERP. The THERP process was properly implemented, and the HEP value appears to be consistent with typical values in other PRAs for human error in alignment of valves.

The generally limited scope and depth of the pre-initiator analysis is a weakness of the licensee's HRA in that it limits the opportunity for the licensee to gain an understanding of the impact that such errors may have on plant risk and of the factors that influence the likelihood of such errors.

E.3.2 Post-Initiator Human Actions.

The post-initiator HRA addressed both response-type and recovery-type actions. The process employed by the licensee to identify and select the post-initiator actions included review of other PRAs, review of Millstone 2 operating procedures, discussion with operations/training staff, review of plant experience, and simulator observations. Numerical screening values suggested in an Appendix to the EPRI SHARP documentation were employed in the initial quantification. Where the licensee judged it to be necessary and justifiable, more detailed analysis was applied to obtain a refined (usually lower) estimate of the operator error probability, and/or additional (recovery) actions were included in the model. Some of the screening values suggested by SHARP (ranging from 1.3 E-03 to 1.3E-01) are significantly lower than are typically used for post-initiator actions (e.g., 0.5). The "cutoff" value for eliminating cutsets from further

consideration was 1E-09/yr, which is not unreasonable, but is generally toward the upper end of the normal range. Thus there is some possibility that important cutsets were eliminated by using the lower screening values. It was not possible for us to determine from this document-only review whether or not the use of these lower screening values had any significant impact on the results of the IPE.

Human actions included in the IPE model were treated as consisting of a "cognitive" response (referred to as an OA type of action) and an action phase (referred to as an HI type of action). The OAs were quantified using one of three time reliability correlations (TRCs): 1) the Human Cognitive Reliability (HCR) model, 2) the EPRI-sponsored Operator Reliability Experiments (ORE) method based on the HCR model, or 3) the Operator Action Tree (OAT) TRC. In all three of these models, the primary determinant of the estimated error probability is the relative time available for operator cognitive response. The licensee states that estimated response times for operators were based primarily on simulator observations. Details of the process for collection of data from simulator observations were not provided. Samples of timing estimates provided by the licensee appear to be reasonable, based on our judgment with limited knowledge of plant-specific procedures and requirements. The licensee indicates that, in addition to response time, performance shaping factors considered included the control room interface, stress level, and the type of behavior (i.e., skill, rule, or knowledge-based). The licensee states that plant-specific assessments performed in support of the evaluation of these performance shaping factors included examination of control room design, plant walkdowns, and observance of accident scenarios in the simulator. No details are provided regarding these plant-specific assessments. In general, the approach used by the licensee to quantify the cognitive response HEPs is similar to approaches that have been used in some other accepted PRAs. Based on the limited information available from the licensee, it appears to us that the depth and rigor of the plant-specific assessment supporting the quantification was relatively limited. However, that judgment may reflect simply a lack of documentation rather than a weakness in the analysis.

Quantification of the HIs was performed using a fault tree representation to decompose the human action of interest to more basic human actions and then using the THERP tables to obtain values for the basic human errors comprising the fault tree. The quantification considered the quality of control room human design (a subjective rating of good, fair, or poor) and "stress level" as performance shaping factors potentially modifying the basic HEPs obtained from the THERP tables. Based on an example data worksheet provided by the licensee, it appears that the appropriate THERP tables were selected. The use of the fault tree representation rather than a THERP tree (or event tree) can be problematic in that it makes it difficult for the analyst to account for sequence-specific variations and dependencies. Typically, it leads to a more "mechanistic" analysis, which tends to limit the understanding of human performance impacts. As noted with for the quantification of OAs, the information available from the licensee suggests the plant-specific evaluation was limited in depth.

A number of recovery actions were identified after the initial quantification and added into the models, in some cases to reflect modeling changes or plant changes after the initial quantification, in other cases simply to credit additional operator recovery actions that were identified as credible and necessary based on a detailed review of initial quantitative results. Apparently, these additional recovery actions were added back into event trees or fault trees, rather than to individual cutsets. Because recovery actions often are very sequence/situation-specific, they usually are incorporated at the cutset level. When added to fault trees, there is a potential that the HEP can appear in inappropriate sequences, or may be combined with other human actions without consideration of dependencies that exist between the human actions. In response to an NRC RAI regarding this issue, the licensee noted that a detailed review of sequences was performed after the addition of the recovery actions to identify inappropriate credit for recovery, including quantitative assessment in which all recovery actions were set to 1.0. The licensee stated that this quantitative assessment had been done recently (presumably since the original submittal of the IPE) and that some questionable combinations were identified. The licensee does not believe that these results alter their conclusions regarding significant core damage sequences. The licensee further states that in the next model update, dependencies among multiple operator actions within individual sequences will be further evaluated. No details regarding these post-submittal results were provided by the licensee. Therefore, we are unable to comment on the licensee's conclusions. Based on the limited discussion presented by the licensee, it appears that dependencies among multiple operator actions were, in general, not accounted for. The lack of a treatment of dependencies among multiple human actions is considered a weakness of the analysis because it could lead to overly optimistic estimates of credit for operator action. It is not possible from this document-only review to assess the significance of this weakness.

E.4 Generic Issues and CPI

The licensee addressed Unresolved Safety Issue A-45, Decay Heat Removal (DHR). A list of special features and capabilities of Millstone 2 which enhance DHR reliability were presented by the licensee, including: 1) a means to use fire water system pumps as an alternate source of auxiliary feedwater suction supply; 2) Emergency Operating Procedures that direct operators to use condensate pumps for feeder flow in the event of a loss of both main and auxiliary feedwater; and, 3) containment air recirculation fan cooler units that provide an alternate means of decay heat removal in the event of loss of shutdown cooling heat exchangers.

The licensee addressed recommendations of the Containment Performance Improvement (CPI) Program related to the vulnerability of the containment or equipment to local or global hydrogen combustion. No vulnerabilities were identified.

E.5 Vulnerabilities and Plant Improvements

The licensee did not employ a specific definition or quantitative criteria to identify a vulnerability. The licensee did identify five "qualitative" criteria that would be consistent with the licensee's concept of a major vulnerability. No vulnerabilities were identified by the licensee using these qualitative criteria. A potential vulnerability that is being actively investigated by the licensee is an interfacing system loss of coolant accident (ISLOCA) resulting from a reactor coolant pump thermal barrier tube rupture. A supplemental report is planned by the licensee upon completion of this evaluation.

E.6 Observations

The following observations are pertinent to NRC staff's determination of whether the licensee's submittal meets the intent of Generic Letter 88-20:

(1) The documentation of the HRA presented by the licensee was weak in comparison to most HRAs reviewed to date. The original submittal discussion of the HRA was extremely abbreviated, to the point that a review of HRA methodology was impossible. Licensee responses to the NRC RAI provided sufficient information to complete our review, though details were still relatively limited. Most of the information about the licensee's approach was derived from or inferred from the licensee's response to the RAI.

(2) 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.

(3) 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.

(4) The licensee's analysis of pre-initiator human actions was relatively weak. Calibration errors were, with the exception of failure to re-open root valves after calibration, dismissed without substantial justification. The treatment of restoration errors was limited in scope and depth. This weakness, in our view, limits the ability of the licensee to identify factors contributing to human error (and therefore plant risk) and to identify possible enhancements.

(5) The treatment of post-initiator human actions used accepted methods, and at a general level appears to have properly applied the selected methods. The post-initiator HRA included both response-type and recovery-type actions. The process for identification

and selection of post-initiator human actions included review of procedures and discussion with plant operations and training staff. Several potentially significant weaknesses in the quantitative analysis were identified:

- Use of relatively low HEP screening values used in the initial quantification may have led to elimination of sequences which warranted further examination

- Use of an essentially generic analysis approach that does not account for sequence and context-specific influences on human behavior and thus limits the ability for the licensee to obtain useful insights on human performance in severe accidents

- Lack of treatment of potential dependencies among multiple operator actions in a sequence may have resulted in overly optimistic results for some sequences.

(6) The submittal included results of importance calculations which identified important human actions.

(7) The licensee used qualitative criteria as guidelines to identify potential vulnerabilities. No vulnerabilities were cited. One potential vulnerability, related to ISLOCA was identified by the licensee as under continuing evaluation.

(8) No human-performance-related enhancements were identified by the licensee resulting from the IPE. The licensee noted several enhancements that had been made as a result of the original Millstone Unit 2 Internal Events PRA that was completed in 1991. Those enhancements were credited in the IPE.

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 Millstone Nuclear Power Station Unit 2 Individual Plant Examination (IPE) submitted by Northeast Utilities (NU) 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 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 and finalize conclusions.

Findings and conclusions are limited to those that could be supported by the document-only review. No visit to the site was conducted. 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. The review addressed the reasonableness of the overall approach with regard to its ability to permit the licensee to meet the goals of Generic Letter 88-20.

1.2 Plant Characterization

The Millstone Unit 2 plant is a Combustion Engineering (CE) pressurized water reactor (PWR) with a power rating of 2,700 MWt and 863 MWe. It is a two-loop plant, with each loop including a steam generator and two reactor coolant pumps. Initial operation was in December, 1975. Design features of particular significance with regard to operator action include:

- Automatic switchover of ECCS from injection to recirculation
- Ability for bleed-and-feed operation
- Fire water backup for Condensate Storage Tank (CST)

2. TECHNICAL REVIEW

2.1 Licensee IPE Process

2.1.1 Completeness and Methodology.

The submittal information on the HRA process was extremely sparse. Additional information submitted by the licensee in response to an NRC request for additional information (RAI) provided sufficient information to complete the document-only review but was still abbreviated and limited. The HRA approach employed by the licensee focused on post-initiator human actions (those taken in response to an accident event) but did address to a limited extent pre-initiator human actions (actions during maintenance, test, etc.) that could cause failure of important equipment on demand during an accident. Quantification of pre-initiator human error was limited essentially to errors in restoration of valves after maintenance. Calibration errors were dismissed without a thorough justification. The post-initiator analysis addressed both response-type actions (anticipated actions in response to an accident event such as those designated in emergency operating procedures), and recovery-type actions (those involving alternative responses or recovery of failed equipment). Cognitive and action phases of operator response were quantified and modeled separately. Quantification of the cognitive portion was performed using one of three published time reliability correlations. Quantification of the action phase was performed using fault trees and tables of basic values from THERP (Ref. 1). Several performance shaping factors were considered for both types of actions, but the plant-specific assessment appears to have been limited in depth and detail. The licensee apparently did not treat dependency among multiple actions in the same sequence.

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

Two other reactors are co-located with Millstone 2. Millstone 1 is a boiling water reactor. Millstone 3 is a Westinghouse PWR. Shared systems and facilities include the 345 KV switchyard and fire protection systems. There is a 4,160 Vac electrical feeder connection between Units 1 and 2. Units 1 and 2 instrument air systems can be cross-connected. The front-end reviewers examined these shared systems and the licensee's accounting of multi-unit effects as part of their review and concluded that the IPE analysis properly accounted for multi-plant interconnections and shared systems. Virtually no information is available from the IPE regarding any human-performance related aspects of the multi-unit operation that could have a significant impact on the IPE results.

The submittal indicates that NU has confidence that the IPE represents the as-built as-operated plant because of the utility's "Living" PRA program, which has evolved to include PRAs for four plants. The submittal (Table 5.4-1) identifies a number of specific activities conducted since 1988 that involved applications of PRA in support of plant activities such as safety evaluations,

prioritization of important equipment and systems, and plant/procedure modifications. This frequent "exercise" of the PRA model and periodic updates of the model, plus the fact noted above that the Level 1 PRA was performed "in-house" by utility personnel, are cited as helping to assure that the current IPE model is a faithful representation of the current plant. Additional factors associated with the living PRA program that are cited as helping to provide this assurance are:

1) Model changes have been fully documented.
2) Past design changes have been systematically screened to identify necessary PRA model updates.
3) A formalized procedure exists for review of all new projects (for implications to the PRA model).
4) The PRA staff has ready access o controlled plant procedures, including Emergency and Abnormal Operating Procedures, and to Licensee Event Reports and Plant Incident Reports.

The submittal discussion of documentation review specifically supporting the IPE is very limited. Section 2.4 of the submittal, "Information Assembly", cites the Final Safety Analysis Report as a source of information on plant layout, and notes that insights from previous NU PRAs - Haddam Neck, Millstone 3, and Millstone 1 - were considered when updates were made to the Millstone 2 PRA. The submittal notes that " Plant walkthroughs and interaction with plant operations personnel are routine activities whenever situations at the plant require the PRA section of NU. NU PRA personnel have also made extensive use of the plant-specific control room simulator." No details of the simulator observations are reported in the submittal.

2.1.3 Licensee Participation and Peer Review.

2.1.3.1 Licensee Participation. The IPE program organization is briefly summarized in Section 5.1 of the submittal. Technical management of the IPE was provided by Northeast Utilities Service Company (NUSCO). The Project Engineer was a member of the Probabilistic Risk Assessment (PRA) section. Contractor support was provided by EQE International for the Unit 2 containment structural analysis, and by Gabor, Kenton and Associates for the Level-2 analysis. The submittal states that all of the front-end analysis and 80% of the back-end analysis was performed by NU personnel. The IPE report was prepared entirely by NU staff, and the Millstone Unit 2 IPE Project Engineer was responsible for review of the overall report write-up. The submittal does not provide specific information on the individuals performing or participating in the HRA. For example, there are no specifics provided that indicate the degree of involvement by plant personnel from operations, maintenance, training, etc., though there are general statements made that discussions/review with operations/training staff were conducted as part of the HRA process.

2.1.3.2 Peer Review. The submittal (Sections 5.2 and 5.3) very briefly summarizes the independent in-house review conducted by NU. For the back-end analysis, independent review was provided by a subcontractor (Gabor, Kenton and Associates); and, for the containment structural analysis, independence was maintained by having the analysis and review performed by two different organizations, one of which was a subcontractor (EQE International). The front-end portions of the IPE report were reviewed by "Cognizant personnel at NU, including Unit Engineering, Project Services Department, Nuclear Licensing, Civil Engineering, and PRA." The IPE analysis was required to follow established utility procedures for independent review. The submittal states that availability of qualified PRA staff was sufficient to assure independence of reviewers. All review comments and resolutions were documented with the calculations. Human reliability analysis is included among the list of general front-end areas reviewed, but few details are provided regarding the review process or results. One of the three review comments identified in the submittal involved identification of a non-conservative value assigned for one human error probability. The HEP of 2.0E-03 used in the model should have been 2.0E-02. The licensee response to the reviewer comment noted that use of the correct HEP value would result in a 3-4% increase in the estimated CDF, and that the correction would be made in the next update of the Millstone 2 PRA model. This comment provides some indication of effective quality assurance review by the licensee.

2.2 Pre-Initiator Human Actions

Errors in performance of pre-initiator human actions, such as failure to restore or properly align equipment after testing or maintenance or calibration of system logic instrumentation, 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 events, how potential events 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 licensee states (in response to an NRC RAI) that pre-initiator human actions considered in the IPE HRA included: 1) Failure to restore or properly re-align equipment after maintenance or test outage, and, 2) Calibration of instruments. The material presented by the licensee addresses only one potential system unavailability related to calibration error, namely the failure to reopen root valves after calibration of the Refueling Water Storage Tank (RWST) level sensor channels. Actually, this is a "restoration" error rather than a miscalibration. The licensee states that, "The likelihood of gross miscalibration is very small,

since there are multiple means of detecting a calibration error, and therefore miscalculation [miscalibration ?] is not considered." Thus it appears that miscalibration per se was ruled out as a significant source of human error in the Millstone 2 analysis. No justification beyond the above quote is provided by the licensee. Miscalibration errors have been significant in some PRAs and, in our view, should not be dismissed without a firm justification. Regarding the failure to restore root valves after calibration of the RWST level sensors, the licensee's response to the NRC RAI included a discussion of the analysis of that error which is discussed further below in Section 2.2.4.

The material presented by the licensee regarding pre-initiator human errors of restoration indicate that the analysis was restricted to failure to restore valves, and perhaps was limited further to a the single case of failure to properly restore (reopen) six manual valves in the high pressure safety injection (HPSI) system after maintenance. The case of the HPSI valves is the only information presented by the licensee. It is not clearly stated by the licensee, but this appears to be the only case of restoration errors treated quantitatively and included in the IPE model.

In summary, the licensee states that pre-initiator human actions related to both calibration and restoration were treated, but the information presented by the licensee indicates that most potential pre-initiator human errors were either not considered or were dismissed as insignificant based on subjective judgment. The scope of actions treated quantitatively and specifically in the model appears to be limited to two specific cases of failure to restore valves to their proper position after maintenance or calibration.

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

The key concerns of the NRC staff review regarding the process for identification and selection of pre-initiator human events 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 material presented by the licensee in the original submittal and in the response to the NRC RAI does not address this issue directly. The material submitted consists of discussion of the two cases of valve restoration noted above for RWST level sensors and for HPSI lines. Specific information regarding the process used to identify all potential pre-initiator errors of significance and then to evaluate those candidate actions to select the ones that warranted further case-specific analysis or quantification is not discussed directly. The licensee does

make the general statement that the HRA approach followed the SHARP (Ref. 2), which does include general guidance for identifying and evaluating potentially significant human actions. Further, the licensee's general discussions of the HRA process indicate that procedures were reviewed and that discussions were held as necessary with operations/training personnel. Specific information that would permit a general assessment of the level of rigor and detail of this qualitative analysis is not provided in the materials presented by the licensee.

2.2.3 Screening Process for Pre-Initiator Human Actions.

It appears that quantification of pre-initiator human actions was limited to the selected cases noted above that were judged to be potentially significant contributors, and that no numerical screening process was employed. Nominal, or final, HEP values were identified for those selected human actions and those values were incorporated into the initial model quantification.

2.2.4 Quantification of Pre-Initiator Human Actions.

Quantification of pre-initiator human actions appears to have been limited to the two cases described below:

a) RWST Level Sensor Miscalibration. As noted above, true miscalibration errors were not included in the model because gross miscalibration was deemed to be very unlikely. While it may well be the case that gross miscalibration errors are very unlikely, the material presented by the licensee does not suggest that the licensee's assertion is supported by a thorough assessment. The potential error that was treated for RWST level sensor miscalibration is restoration of the isolation (root) valves after calibration, because it was considered to be a "credible mode of system failure." The licensee discusses a number of reasons why this failure is unlikely, including four different specific procedures that direct monitoring, verification, and surveillance checks which be expected to detect the failure during startup and/or operation. The licensee noted that, although not typically done, calibration might be performed during operation. This would eliminate credit for verification during startup. The licensee further assumed dependency of the failure to open valves for multiple channels (i.e., if the technician failed to reopen the valve after calibration of one valve, that technician likely would fail to open the valves for the other channels). These assumptions appear to be appropriately conservative. A failure probability for failure to close the one valve was determined using THERP. Details of that analysis, e.g., specific tables for the basic HEPs, performance shaping factors applied, or credit for recovery by independent checks, are not provided by the licensee. The HEP value reported, 1.44E-03 is a credible value; i.e., it is in the general range of values used in other PRAs for apparently similar actions.

This probability of failure to restore the valves was then multiplied by the ratio of the detection time to the time between calibrations. The licensee assumed that if the valves were left unopened they would be detected within four hours of operation after the error. This assumption was based on the fact that procedures require operators to check once per shift that all four RWST level channels agree within 4% level. Since that check could be performed at any time during the shift, an average detection time of 4 hours was assumed. Since calibration is performed once per cycle, or every 18 months, the probability of failure was multiplied (reduced) by a factor of 4hrs/18months; i.e., from 1.44E-03 to 4.4E-07. This assumption that the error would be detected within four hours may be optimistic. However, we do not have the details of the instrumentation involved, the procedures, or the control room practice which would permit judgment on the appropriateness of this assumption regarding detection. It does appear that if the valves were left closed the reading in the control room would be zero level in the RWST, and that this indication would be likely to be detected by the control room operators; if not during the first shift, then soon after as shifts change. In our view, it would be prudent to first determine if a less optimistic assumption regarding detection of the error would have a significant impact on the likelihood of core damage, and then if necessary perform a more rigorous assessment of the likelihood of detection and the overall expected error probability.

b) Failure to Restore Valves. The licensee's discussion of treatment of restoration errors consisted of a description of the approach to quantification of failure to reopen six normally-locked-open manual isolation valves in the HPSI system (two each in the suction lines, discharge lines, and recirculation lines) after maintenance. Failure to reopen these valves could disable a portion of the HPSI system. The human error probability for failure to restore these valves was calculated using THERP to be 4.2E-04. The THERP tree and THERP tables used to calculate this value were presented by the licensee as part of their response to the NRC RAI, and the calculations appear to have properly employed the THERP guidance. Credit was appropriately assigned for independent checker using a checklist. No other performance shaping factors appear to have been considered directly. As in the case of the RWST root valves, this human error probability was multiplied by the ratio of the expected detection time to the time between maintenance actions (opportunity for error) in order to obtain an estimate of the overall contribution to unavailability of the HPSI system on demand due to this pre-initiator human error cause. In this case, it was assumed that HPSI maintenance would be performed on line and on demand (as detected through monthly maintenance activities or otherwise). The estimated (corrective) maintenance frequency (the inverse of time between maintenance) was estimated from plant data to be 5.84E-04 events/hr (41 events over a 70,200 hour period). It was assumed that the detection time would be, on the average, one-half of the time between required routine surveillance; i.e., 1/2 of 720 hr, or 360 hours. Therefore, the HEP was reduced by a factor of (360 x 5.84E-04 = 0.21); from 4.2E-04 to 8.85E-05. Again, we do not have the details of the procedures, etc. to determine whether the licensee's assumptions regarding detection of

the error are appropriate. It is reasonable to take credit for proceduralized actions such as required surveillance checks that would detect latent errors. It is not possible for us to determine from this document-only review whether the licensee's assumptions are appropriately conservative.

Overall, the information available from the licensee regarding the assessment of pre-initiator human errors indicates that the assessment was relatively narrow in scope and limited in depth. Calibration errors were discounted without a thorough justification being presented. The scope of the assessment of restoration errors was limited to valves, and apparently to a single case of the HPSI valves. The THERP calculation presented by the licensee appears to have been properly executed, though not particularly detailed. While this general weakness of the pre-initiator analysis may or may not have a significant impact on the gross quantitative results of the IPE or the basic conclusions from the study, it does limit the potential for the licensee to gain a full appreciation of the ways in which human performance can influence overall risk and to identify potential risk reduction measures. In some PRAs more rigorous assessment of pre-initiators has determined that they are a significant contributor to risk, and some enhancements have been made which have contributed to an overall estimated reduction of risk based on the assessment of pre-initiator actions.

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 failing to perform required activities as directed by procedures, can have a significant effect on plant risk, and in some cases have been shown to be dominant contributors to core damage frequency (CDF). These errors are referred to as post-initiator human errors. Our review determines 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 PRAs: response-type actions, which include those human actions performed in response to the first level directives of the emergency operating procedures/instructions (EOPs, or EOIs); and, recovery-type actions, which include those performed to recover a specific failure or fault (primarily equipment failure/fault) such as recovery of offsite power or recovery of a front-line safety system that was unavailable on demand earlier in the event. The Millstone 2 HRA addressed both response-type and recovery-type actions per the above descriptions. It appears that most or all of the response actions were incorporated into the IPE model as basic events in fault trees, though some of the top events in the event trees (e.g., bleed and feed) are dominated by the human action. Some

recovery actions were identified after initial quantification and placed in fault tree and event tree models for subsequent requantification. The more usual practice is to examine the applicability of recovery actions on a cutset-specific basis and to add the recovery actions to specific cutsets as applicable. Placing additional operator actions back into fault trees or event trees can lead to unrealistic compounding of credit for operator action, particularly if dependencies among multiple operator actions are not accounted for (which appears to be the case for the Millstone 2 HRA). This issue is discussed further below.

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 associated with the accident sequences delineated and the systems modeled; and, (2) discussions were held with appropriate plant personnel (e.g., operators, shift supervisors, training, operations) 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 provides limited direct discussion of the process for identification of human errors to be included in the IPE model. However, there are general statements in a number of discussions in the submittal indicating that procedures were reviewed and that personnel were involved in identification and review of operator actions. The licensee's response to an NRC RAI states that the general approach to organization of the HRA task was a modification of the SHARP procedures developed by EPRI (Ref. 2), and that steps 1 and 2 of the SHARP process, which are designed to assure that important human actions are included in the PRA model, were followed. In addition, the licensee states that identification and selection of operator actions included: 1) review of emergency procedures; 2) discussion with plant operators; 3) discussion with plant operator trainers; 4) review of past PRAs; 5) simulator runs; and, 6) actual special initiators which had been experienced by Millstone 2. No further details were provided by the licensee, but this general description indicates that the licensee's process was structured to provide reasonable assurance that post-initiator actions of major importance were not overlooked. We did not identify important operator actions typically included in other PRAs for similar plants that were overlooked.

2.3.3 Screening Process for Post-Initiator Response Actions.

The licensee employed as set of screening values recommended in an appendix to the SHARP documentation (Ref. 2). These screening values were not intended to be used to eliminate operator actions from the model. Operator actions were screened "qualitatively" as described

above. All operator actions identified in that qualitative process were quantified using either screening values from SHARP, or using "nominal" HEP estimates from one of the HRA methods identified below.

The screening values from SHARP depend on the designation of the particular action as "Skill-Based", "Rule-Based", or Knowledge-"Based" as follows:

Skill-Based	1.3E-03
Rule-Based	1.3E-02
Knowledge-Based	1.3E-01

A decision tree was used to classify an action as skill-, rule-, or knowledge-based. The blocks in the decision tree address whether:

- The operation was "routine"
- The transient or operation is likely to be unambiguously understood by the operator
- A procedure is required
- The procedure covers the case in question
- The procedure is well written
- The procedure is understood by the personnel
- Personnel are well practiced in the use of the procedure.

Screening values typically used in PRAs are higher than these EPRI values. (For example, a value of 0.5 is more typical for response type actions.) While the licensee did not use the screening values to eliminate specific operator actions, use of lower screening values may eliminate important sequences from consideration. The "cutoff" value used in the Millstone analysis for including/excluding cutsets was 1.0E-09/yr. This is a reasonable, but relatively high cutoff value in comparison to many PRAs. Further, it appears that the Millstone HRA did not address possible dependencies among multiple human actions in a given cutset. Therefore, there is some potential that cutsets were eliminated, or that important human actions were not investigated in depth, because the initial quantification using the lower screening values did not identify the sequence as important. It is not possible to determine from this document-only review the impact that use of these lower screening values had on the Millstone 2 IPE results.

2.3.4 Quantification of Post-Initiator Human Actions.

Where more detailed modeling was required (i.e., for operator actions in dominant sequences), the operator action was treated as consisting of two "groups" corresponding to "cognitive" tasks of detection, diagnosis, decision actions (OA) and "physical" tasks associated with equipment manipulation (HI). The cognitive tasks are referred to as OAs; the physical tasks, as HIs. The OAs and HIs were treated as individual human actions (basic events) and were combined using

the fault tree linking methodology employed for the IPE modeling. Note that in general, the OA and HI are treated as independent actions. Further, this treatment of operator actions in fault trees severely limits the potential to model the sequence-specific dependencies of human behavior. Human actions are treated as part of equipment fault trees, which are automatically called into the model whenever that equipment is addressed, regardless of the context of the human action. The likelihood of human action is in general highly dependent on the context of the situation. In its response to an NRC RAI, the licensee states that since the IPE submittal was made in 1993, they have started using state-of-the-art PC based PRA codes which can accommodate sequence-dependent operator actions, and that current plans are to enhance the post-initiator HRA method in the next update of the Millstone 2 IPE.

2.3.4.1 Quantification of Cognitive Actions. OAs were quantified using one or more of three time reliability correlations:

The Human Cognitive Reliability (HCR) Model (Ref. 3)
ORE/HCR Method (Ref. 4)
OAT/Time Reliability Correlation." (Ref. 5)

The licensee indicates that typically the HEP was calculated using two or three of the models and then select the final value based on the analysts judgment of the most appropriate data and model. (Obviously, the value calculated was considered as part of the judgment process.) In these time reliability correlations, the primary determinant of the HEP value is the relative time available for the operator response. The type of action (skill-, rule-, or knowledge-based) affects the choice of correlation in the HCR models, and therefore can be considered a performance shaping factor (PSF). In addition, the licensee indicates that control room interface and stress level were assessed and used to modify HEPs. Based on an example provided by the licensee, it appears that control room interface was subjectively rated "good", "fair" or "poor" and that stress levels were subjectively rated "low", "normal", "potential", or "grave". The information provided by the licensee is not sufficient to determine the quantitative impact on the HEP corresponding to these subjective ratings. In response to an NRC RAI, the licensee states that, "The plant specific assessments performed to evaluate the PSFs included examining [the] control room design, performing plant walkdowns, and observing scenarios in the simulator runs." Essentially no further information is presented by the licensee regarding the process for quantification of OA type post-initiator human actions.

As noted above, the HEP values from the time reliability correlations depend primarily on the estimated timing (time available vs. time required) for the operator "cognitive" action. The submittal states that the time available to prevent core damage (task performance time) was based on plant-specific thermal hydraulic analyses; and that the time required (median task time) was, "Based on plant-specific simulator data, reports and conversations with operators and trainers •••." Two industry reports (Ref. 4 and Ref. 6) were used as "starting points" to obtain

median task times. Engineering judgment was used to assure that the data in the reports are applicable to Millstone 2. In a response to the NRC RAI, the licensee states that most of the time data came from a simulator observation rather than from operator interviews.
Regarding simulator exercises, the submittal notes that PRA personnel were able to observe simulator exercises during normal operator training and through exercises scheduled specifically for the HRA. Two PRA personnel observed simulator exercises. Typically a scenario of interest was observed four or five times with different operator crews. Overall, approximately thirty simulator runs were observed in support of the Millstone 2 HRA. The submittal notes that these observations provided perspective on the use of procedures, control room (human-machine) interface, and operating crew variability, as well as median task times for input to the time reliability correlations.

2.3.4.2 Quantification of Physical Actions. The submittal states that, "The HI covered not only control board operations but also the actions of the auxiliary operators. Human reliability fault trees were developed to model specific HIs. For the HI quantification, failure probabilities from NUREG/CR-1278 were input to the HRA fault trees." As noted by the licensee, this approach cannot really be said to use the THERP methodology in that it does not employ "THERP trees". Operator actions of interest that appear as basic events in the overall model fault trees or event trees were broken down into more elemental actions using a fault tree format rather than a THERP tree. Basic HEPs for the elemental actions were obtained from THERP tables. These basic HEPs were modified to account for selected performance shaping factors (apparently control room interface and stress), and the overall HEP is calculated from the fault tree logic. Numerically, the two formats (fault tree and THERP tree) can be equivalent. However, many analysts find that the THERP tree format, which is more like an event tree, makes it easier for an analyst to identify and account for sequence-specific variations and dependencies in HEPs. The Millstone 2 approach using fault trees does not account for such dependencies, which is a limitation of their approach.

2.3.4.3 Quantification of Recovery Actions. The licensee identified (in a response to an NRC RAI) seven recovery actions that were identified and added to the model after the initial quantification. HEP values for most of them were identified in the submittal in Table 3.4.1-3, which is a listing of importance values for modules/components in the IPE model. The seven recovery actions and, where identified, the HEP values are listed below in Table 2-1. Some of these recovery actions were added to the model because review of dominant sequences indicated that credit for operator action was necessary and appropriate. Some were added as part of modeling changes which were made to reflect plant changes or simply different modeling assumptions. The information presented by the licensee does not discuss any different approach used to quantify recovery actions, and we assume that the time reliability correlations used for response-type actions were applied.

Table 2-1
Recovery Actions

Identifier	Action Description	HEP Value
OAESASREC	Manual initiation of ESAS actuated equipment, loss of SWGR ventilation (small-small, small, and medium break LOCA)	3.76E-03
OADCV	Cognitive error to recover DC SWGR ventilation	1.56E-02
OAFAN	Operator recovery of ESF Room ventilation	3.70E-02
OARTM	RWST makeup (SGTR)	None ID [1]
RECSC	Recovery of RBCCW or SW (RCP seal LOCA)	1.87E-02
OATRC	Operator action to trip RCPs (Loss of SW and Loss of RBCCW events)	8.72E-03
MFW1	Recovery of main feedwater	None ID [2]

[1] RWST inventory makeup following a SGTR was listed as an apparent response-type action with an HEP = 1.3E-03.
[2] Recovery of main feedwater was listed as an apparent response-type action with an HEP = 1.3E-03; may or may not be the same action.

The HEP values are generally consistent with values used for the response-type actions included in the initial quantification. Particular care should be taken in applying the time reliability correlations for recovery actions. The time reliability correlations are based on simulator data for response-type actions. Typically, these actions are proceduralized actions in the Emergency Operating Procedures (EOPs) or Abnormal Operating Procedures (AOPs) and are highly practiced. Recovery actions may or may not be similar, but usually are at least alternative responses and are not the "expected" response to the abnormal event. While some recovery actions were noted as proceduralized, the licensee does not state clearly whether all recovery actions credited are proceduralized, highly practiced actions. The information presented by the licensee does not indicate that the analysis was sensitive to potential differences in context for recovery actions vs. response actions.

Recovery actions were incorporated back into the fault tree or event tree models. Usually recovery actions are found to be highly sequence/situation dependent, and therefore are added directly to specific cutsets rather than included in fault/event trees. Placing them in fault trees, in

particular, makes it difficult to account for these sequence/situation specific dependencies. Further, when recovery actions are included in fault trees, the HEP can appear in multiple sequences and in different combinations with different system failures for which the recovery action is not logical, or is less likely. Recovery actions may appear in combination with other human actions, in which case dependencies among the multiple human actions should be addressed. The licensee's analysis did not address potential dependencies of recovery actions on sequence or context-specific factors or dependencies that might occur between multiple operator actions credited in a given cutset.

In response to an NRC RAI, the licensee indicated that some attention has been given to the issue of multiple recovery actions in a sequence since the submittal of the IPE. The licensee states that:

> "One method that is used to verify that inappropriate multiple recovery actions do not exist is to set all recovery actions equal to 1.0 and review the generated list of core damage sequences. This has been done recently for the MP2 model and some questionable combinations showed up. However, we do not believe that these alter the conclusions regarding significant core damage sequence or their identification. In the next model update, dependencies among multiple operator actions within individual sequences will be further evaluated."

This generally "mechanistic" treatment of recovery actions is consistent with the apparent overall approach to the Millstone HRA, and we believe is a weakness of the HRA. It is not possible to determine the net impact on the overall results of the IPE. In general, the HEP values for the recovery actions are perhaps lower than typical. As noted above, they were derived from the same sources as the response-type actions, and values were consistent with the response actions in the Millstone 2 HRA. (In general, the Millstone 2 values for response type actions are at the high (conservative) end of the range typically seen in other PRAs.) In response to an NRC RAI regarding the estimated overall quantitative impact of credit for recovery actions, the licensee referred to an overall 50% reduction in core damage frequency (CDF) caused by changes in the IPE model, some of which were due to plant changes, and some of which were due to modeling changes. The licensee estimated that approximately 15% to 20% of the reduced CDF estimate was the result of inclusion of operator recovery actions. No details were provided to support this estimate; and, it is not clear that the response fully addresses the issue of the overall impact of inclusion of recovery actions. However, the apparent magnitude of credit for recovery actions is not large in comparison to other PRAs.

2.3.5 Human Actions in the Flooding Analysis.

The flooding analysis considered effects of both spray and immersion of equipment. In the case of the spray analysis, equipment failures were assumed to occur at the time the flood (spray)

initiator occurs, and were assumed to be unrecoverable (no operator action). In the case of flooding due to immersion, operator action in identifying and isolating the flooding source was credited. The analysis apparently considered a combination of three failures in as part of the failure of operator action to identify and isolate the flood source:

1) Failure to recognize the existence of a flooding condition provided by indications during plant walkdowns at the time of flooding (HEP = 0.9)

2) Failure to recognize that flooding is occurring, given an indication or alarm (HEP = 1.0E-02), and

3) Failure to take mitigating measures, despite the fact that a flooding condition is recognized (HEP = 1.0E-02).

The HEP values are intended to be conservative screening values and are based on engineering judgment. The exact logic for combining these three human errors is not presented by the licensee; but for any logical combination of these actions, the overall failure probability is still on the order of 1.0E-02, which is typical of values assumed in other PRAs for operator failure to identify and isolate the source of flooding in time. The Millstone 2 analysis was relatively crude, in that credit for this human action apparently was taken in all cases of flooding by immersion, without case-by-case analysis.

2.3.6 Human Actions in the Level 2 Analysis.

The licensee states that operator actions in the back-end, or Level 2, analysis were represented by "House Events" which could be either true (value of 1.0) or false (value of 0.0), depending on whether or not the front-end analysis credited the recovery action. There were three such operator actions included as house events in the containment event trees (CETs) for the Level 2 analysis:

1) V-FLANGE: Reactor cavity flange (access door) not removed
2) VOPAF-PSR-SRV: Operator does not open pressurizer's PORV
3) VOPAF-2ND-SRV: Operator does not open atmospheric dump valves.

Other than these house events, operator actions were not considered directly in the Level 2 analysis, except for review for accident management considerations.

2.3.7 GSI/USI and CPI Recommendations.

Review of the submittal discussions of Generic Safety Issues (GSIs) and Unresolved Safety Issues (USIs) is primarily the focus of the front-end reviewer. Review of submittal discussions

of any licensee actions in response to Containment Performance Improvement (CPI) recommendations is performed primarily by the back-end (Level 2) reviewer. If the licensee's discussion of these issues has particular significance to the HRA or human performance issues, those points are included in this review.

The licensee addressed Unresolved Safety Issue A-45, Decay Heat Removal (DHR). A list of special features and capabilities of Millstone 2 which enhance DHR reliability were presented by the licensee, including: 1) a means to use fire water system pumps as an alternate source of auxiliary feedwater suction supply; 2) Emergency Operating Procedures that direct operators to use condensate pumps for feeder flow in the event of a loss of both main and auxiliary feedwater; and, 3) containment air recirculation fan cooler units that provide an alternate means of decay heat removal in the event of loss of shutdown cooling heat exchangers.

The licensee addressed the CPI recommendation pertinent to PWR large dry containments regarding evaluation of vulnerabilities of containment and equipment to local and global hydrogen combustion. The licensee concluded from the IPE analysis that:

- Only by assuming 100% cladding oxidation could an early hydrogen burn challenge the containment integrity

- For all accident sequences, the likelihood of deflagration to detonation transition is highly unlikely to impossible

- Global hydrogen burns would be more prevalent than localized burns due to the open design of the containment and natural circulation mixing.

2.4 Vulnerabilities, Insights and Enhancements

2.4.1 Vulnerabilities

The submittal notes that it does not have formal criteria which define a "vulnerability," but that the following criteria would be in line with their concept of a major vulnerability:

1. Single failure of safety- or nonsafety-related equipment which is either active or passive in nature and has significant impact on CDF.

2. Multiple safety- or nonsafety-related components which, because of physical proximity, systems interactions, or environmental consideration, have a high potential for common mode failure and have a significant impact on CDF.

3. A support system which has a relatively high probability of failure, could result in an unanticipated plant transient not covered by procedures, could result in the loss of multiple front-line and support systems, and has a significant impact on CDF.

4. An operator action which has a reasonable probability of being demanded over the plant lifetime, has a moderately high probability of failure because of relatively complex procedures or operator unfamiliarity, and a significant impact on CDF.

5. A mode of early containment failure which has a relatively high probability of occurrence given a core melt accident (i.e., greater than about 10 percent).

Based on the above concepts, the licensee did not identify any severe accident vulnerabilities. One potential vulnerability, reactor coolant pump (RCP) thermal barrier tube rupture leading to a possible interfacing systems LOCA, is being actively evaluated. A supplemental report is planned when this ongoing analysis is completed.

2.4.2 Insights Related to Human Performance.

Section 7.1.1 and 7.1.2 of the submittal summarize major insights from the IPE front-end analysis and back-end analysis, respectively. None of the insights identified relates directly to a human performance issue.

2.4.2.1 Important Human Actions. The submittal presents importance calculations for individual "components", including operator actions. Cognitive error of the operators to manually initiate the steam driven auxiliary feedwater (SD AFL) pump, and failure to recover DC power (which includes operator action) are noted as important contributors to CDF, though not as "vulnerabilities". Failure to initiate the SD AFL pump has a Fussel-Vesely (F-V) importance of 0.161 and is the fourth most important component/module. Failure to recover DC power early and failure to recover by 35 minutes have F-V importance values of 0.194 and 0.180, respectively, and are the second and third most important contributors. No other operator actions are among the top 10 most important contributors. The ten most important operator actions are listed in Table 2-2 below.

2.4.2.2 Human Performance Related Enhancements. No human-performance-related enhancements were identified in the submittal that resulted from the IPE. Section 6 of the submittal identifies five recommendations for plant/operations improvements made as a result to the original Millstone Unit 2 Internal Events PRA completed in 1991. Those five improvements have been implemented and are credited in the IPE. The licensee notes that the overall CDF has decreased by approximately 50% as a result of these improvements. Section 6 of the submittal also identifies two plant changes - modifications to ensure redundancy in feedwater isolation on a Main Steam Isolation signal, and replacement of

Table 2-2
Ten Most Important Operator Actions

HEP ID Import.	DESCRIPTION	HEP	F-V
RDC1	Failure to recover DC power (short term)	2.16E-01	1.94E-01
RDC2	Failure to recover DC power (35 minutes)	4.35E-01	1.80E-01
FQ1PXCP4	Cognitive error; operators fail to initiate SD AFL pump	1.3E-02(1)	1.61E-01
OABAF1	Cognitive error; failure to initiate bleed and feed	1.0E-01	5.303E-02
OAFAN	Operator action to recover ESF Room ventilation (OA & HI)	1.3E-01	3.697E-02
MFWNONRC	Failure to recover MFW given loss of MFW initiating event	1.3E-03(1)	2.245E-02
HIRBLOCAL	Recovery action: failure to locally close RBCCW AOV(s)	1.3E-01(1)	1.595E-02
OADCV	Cognitive error; failure to recover DC Switchgear Room ventilation	1.0E-02	1.558E-02
MMFPREC1	Manipulative error; failure to recover MFW given loss of DC Bus	1.30E-01	1.473E-02
HISWLOCAL	Recovery action; failure to locally open SW AOV(s)	1.3E-01(1)	1.185E-02

(1) HEP identifiers are not provided in the table of HEP values. This value appears to be the correct value for this basic event, but there is some uncertainty. In particular, the tabulated values for HIRBLOCAL and HISWLOCAL include both OA and HI components, while the identifier suggests that the importance value relates to the HI portion only.

steam generators - which are important safety-related improvements but did not directly impact the PRA.

3. CONTRACTOR OBSERVATIONS AND CONCLUSIONS

The intent of the IPE is summarized in four specific objectives for the licensee identified in Generic Letter 88-20 and NUREG-1335:

(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 could 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 and conclusions are pertinent to NRC staff's determination of whether the licensee's submittal meets the intent of Generic Letter 88-20:

(1) The documentation of the HRA presented by the licensee was weak in comparison to most HRAs reviewed to date. The original submittal discussion of the HRA was extremely abbreviated, to the point that a review of HRA methodology was impossible. Licensee responses to the NRC RAI provided sufficient information to complete our review, though details were still relatively limited. Most of the

information about the licensee's approach was derived from or inferred from the licensee's response to the RAI.

(2) 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.

(3) 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.

(4) The licensee's analysis of pre-initiator human actions was relatively weak. Calibration errors were, with the exception of failure to re-open root valves after calibration, dismissed without substantial justification. The treatment of restoration errors was limited in scope and depth. This weakness, in our view, limits the ability of the licensee to identify factors contributing to human error (and therefore plant risk) and to identify possible enhancements.

(5) The treatment of post-initiator human actions used accepted methods, and at a general level appears to have properly applied the selected methods. The post-initiator HRA included both response-type and recovery-type actions. The process for identification and selection of post-initiator human actions included review of procedures and discussion with plant operations and training staff. Several potentially significant weaknesses in the quantitative analysis were identified:

- Use of relatively low HEP screening values used in the initial quantification may have led to elimination of sequences which warranted further examination

- Use of an essentially generic analysis approach that does not account for sequence and context-specific influences on human behavior and thus limits the ability for the licensee to obtain useful insights on human performance in severe accidents

- Lack of treatment of potential dependencies among multiple operator actions in a sequence may have resulted in overly optimistic results for some sequences.

(6) The submittal included results of importance calculations which identified important human actions.

(7) The licensee used qualitative criteria as guidelines to identify potential vulnerabilities. No vulnerabilities were cited. One potential vulnerability, related to ISLOCA was identified by the licensee as under continuing evaluation.

(8) No human-performance-related enhancements were identified by the licensee resulting from the IPE. The licensee noted several enhancements that had been made as a result of the original Millstone Unit 2 Internal Events PRA that was completed in 1991. Those enhancements were credited in the IPE

4. DATA SUMMARY SHEETS

Important Operator Actions/Errors:

The ten most important operator actions and (Fussel-Vesely) importance values are:

HEP ID Import.	DESCRIPTION	HEP	F-V
RDC1	Failure to recover DC power (short term)	2.16E-01	1.94E-01
RDC2	Failure to recover DC power (35 minutes)	4.35E-01	1.80E-01
FQ1PXCP4	Cognitive error; operators fail to initiate SD AFL pump	1.3E-02[1]	1.61E-01
OABAF1	Cognitive error; failure to initiate bleed and feed	1.0E-01	5.303E-02
OAFAN	Operator action to recover ESF Room ventilation (OA & HI)	1.3E-01	3.697E-02
MFWNONRC	Failure to recover MFW given loss of MFW initiating event	1.3E-03[1]	2.245E-02
HIRBLOCAL	Recovery action: failure to locally close RBCCW AOV(s)	1.3E-01[1]	1.595E-02
OADCV	Cognitive error; failure to recover DC Switchgear Room ventilation	1.0E-02	1.558E-02
MMFPREC1	Manipulative error; failure to recover MFW given loss of DC Bus	1.30E-01	1.473E-02
HISWLOCAL	Recovery action; failure to locally open SW AOV(s)	1.3E-01[1]	1.185E-02

[1] HEP identifiers are not provided in the table of HEP values. This value appears to be the correct value for this basic event, but there is some uncertainty. In particular, the tabulated values for HIRBLOCAL and HISWLOCAL include both OA and HI components, while the identifier suggests that the importance value relates to the HI portion only.

Human-Performance-Related Enhancements:

No human-performance-related insights or enhancements were identified by the licensee as resulting from the IPE. Improvements identified previously in the original Millstone 2 PRA that have been implemented in the plant and credited in the IPE were identified by the licensee.

REFERENCES

1. Swain, A.D. and H.E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278-F, August, 1983.

2. Systematic Human Reliability Procedure (SHARP), Palo Alto, CA: Electric Power Research Institute, June 1984, EPRI NP-3583.

3. Hannaman, G.W., A.J. Spurgin, and Y.D. Lukic, "Human Cognitive Reliability Model in PRA Analysis," Draft EPRI report, December, 1984.

4. EPRI-NP-6560-L, "A Human Reliability Analysis Approach Using Measurements for Individual Plant Examination," December, 1989.

5. R.E. Hall, J. Fragola, J. Wreathall, Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation, November 1982, NUREG/CR-3010.

6. Legand, M., A. Villemeu, and A. Obat, "Operation Actions Following Abnormal Transients: Tests or Simulators," Conference on Anticipated Abnormal Plant Transients in Light Water Reactors, ANS Topical Meeting, Jackson, Wyoming, September 26-29, 1983.