CA/TR-94-019-16

KEWAUNEE NUCLEAR POWER PLANT

TECHNICAL EVALUATION REPORT OF THE IPE SUBMITTAL HUMAN RELIABILITY ANALYSIS

FINAL REPORT

P. M. Haas
P. J. Swanson

Prepared for

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Divisiou of Safety Issue Resolution

December 1994

CONCORD ASSOCIATES, INC.
Systems Performance Engineers

725 Pellissippi Parkway
Knoxville, TN 37933

Contract No. NRC-04-91-069
Task Order No. 16

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY

This Technical Evaluation Report (TER) is a summary of the technical review of the human reliability analysis (HRA) presented as part of the Kewaunee Nuclear Power Plant Individual Plant Examination (IPE) submitted by Wisconsin Public Service Corporation (WPSC) to the U.S. Nuclear Regulatory Commission. The review was performed to assist NRC staff in their evaluation of the IPE and conclusion regarding whether the submittal meets the intent of Generic Letter 88-20. The review consisted of a "document-only" review of the submittal and supporting material provided by the WPSC in response to NRC requests for additional information.

General Review

The licensee's HRA approach addressed primarily post-initiator actions, including response-type and recovery-type actions. A limited-scope assessment of pre-initiator human errors was also included. The analysis of post-initiator actions employed a Westinghouse methodology based on the Technique for Human Error Rate Prediction (THERP) described in NUREG/CR-1278 to quantify human error probabilities (HEPs) for selected operator actions identified from the Emergency Operating procedures (EOPs), System Operating Instructions (SOIs), and Abnormal Operating Procedures (AOPs). The licensee's approach incorporates several underlying assumptions regarding improvements to procedures, training, control room human-machine interface, etc., since the development of THERP. The licensee's position is that these improvements require/permit use of less conservative (lower) error probabilities than provided in the THERP Handbook. In our view, the licensee's assumptions, overall, are optimistic, though we recognize that "hard" data is limited, and some of the points are arguable. However, it is important that the licensee's analysis carefully assesses, on a case-by-case basis, the validity of the assumptions and the credit taken for human action, and that the licensee document the basis for these assumptions/credit, particularly since the licensee's position differs from most of the industry. The degree to which the licensee performed such an in-depth assessment is difficult to judge in a document-only review, i.e, without a plant visit and more detailed review of tier-2 documentation. However, the impression gained from our review of the submittal and licensee responses to NRC questions is that the licensee may have applied a number of non-conservative assumptions "across the board", without plant-specific and situation-specific evaluation.

The utility staff were involved in the development of the IPE. Three Kewaunee staff members were assigned to the IPE development team. All three had previous plant operations experience; two had been Shift Technical Advisers (STAs), and one had been a Senior Reactor Operator (SRO) and Shift Supervisor (SS). A Kewaunee group supervisor served as project manager. Westinghouse personnel provided HRA training to WPSC staff, who then performed the HRA. The submittal states that there was support from other departments in the utility nuclear organization, but does not provide specifics of the areas of expertise or roles of the different participants. The submittal states that because of this involvement, in particular the active involvement of the two STAs through most of the

project, that formal systems walkdowns were not necessary. In response to an NRC request for additional information, the licensee indicated that in the event of any doubt on the part of the STAs, an informal walkdown was performed on the system or system part in question. Further, the licensee noted that detailed walkdowns were performed for internal flooding and Level 2 analyses, and that SROs from Operations and Training reviewed fault trees and system notebooks to assure they represented the as-built configuration. The licensee indicated that plant modifications, Technical Specifications and procedural changes up to the submittal date of 12/1/92 were reflected in the IPE model, with some exceptions related to failure/unavailability data with an end date of December, 1989. The direct involvement of operations staff, combined with informal walkdowns and document review appears to have comprised a reasonable process for assuring that the plant represents the as-built, as-operated plant.

The licensee conducted an internal review of the IPE. The review team was composed of nine members from Operations, Plant Engineering, Maintenance, and Training Departments, all with plant operations experience. Five of the members were licensed SROs; four were STAs. The review process resulted in more than 450 separate comments. Some technical comments resulted in procedures modifications; others resulted in insights deferred until implementation of the planned accident management program. In addition to this internal staff review, an independent review was provided by contract personnel from Battelle, Safety Management, Inc., Sargent & Lundy, and Wisconsin Electric. Areas of expertise on the external review team included Level 1 PRA, Level 2 PRA, and HRA. The review addressed methodology and overall project quality. The submittal states that in-depth review was provided in areas (including HRA) in which in-house expertise was limited. No specific review comments regarding the HRA review were provided. The combined internal and external review process provided additional assurance of the technical accuracy of the IPE model.

Pre-Initiator Human Actions

The HRA included only a very limited-scope assessment of pre-initiator human actions, i.e., human actions during maintenance, test or calibration that could disable a system. There was no discussion provided in the submittal of a pre-initiator analysis, though two pre-initiator actions were quantified. In response to an NRC request for additional information, the licensee indicated that pre-initiators had been considered qualitatively and generally, and with a few exceptions, had been dismissed from further consideration or quantification. Regarding operator actions to restore equipment after test or maintenance, the licensee states that, "In most cases, the failure of these steps would result in either an annunciator or a status light in the control room to light, alerting the control room operator to such a condition. Shift changes every 12 hours would also have a high probability of detecting such an error. Therefore, these errors are not considered in the HRA." Calibration errors were dismissed without plant-specific assessment because, "They have seldom been shown to be important in past PSAs." The only pre-initiator actions assessed were restoration of manual valves that are used to disable a system's safeguard function during test and maintenance. The licensee's

response indicates that all such valve restorations were modeled; none were screened out. However, as indicated above, our review identified only two pre-initiators quantified. Pre-initiator actions, including miscalibration, have been identified as important contributors in some PRAs, and should not be dismissed without careful, plant-specific, assessment. Inadequate consideration of pre-initiator human errors may lead to overly optimistic estimates of sequence contributions to CDF, and/or to missed insights regarding human performance contributions to risk.

Post-Initiator Human Actions

As indicated above, the HRA considered both response-type and recovery-type post-initiator human actions. Identification and selection of operator actions to be quantified was based on a review of procedures. The process was not well described in the submittal, but in response to an NRC request for additional information, the licensee provided summary information that indicated a reasonably thorough review process was employed. An initial review was performed by a WPSC HRA analyst (an engineer with STA training), a Westinghouse HRA specialist, and a WPSC SRO. Subsequently, the HRA notebook was reviewed by at least one SRO as part of the internal review process described above. The reviews consisted of analyzing each procedure step in terms of the success criterion for a given fault tree. Only those steps that, if failed, would cause the success criterion not to be met, were considered. Recovery actions were modeled only if they had a major impact on the plant CDF (i.e., more than about 10%), and only if there were symptom-based procedures in place or planned to direct the operators to the required action. Actions modeled are generally consistent with actions modeled in other PWR PRAs.

No numerical screening process was employed to identify more critical actions and eliminate less important ones from further consideration. All actions identified were quantified and included in the IPE model. Human actions at the functional level are identified through proceduralized tasks tied to the particular accident sequence being considered. These actions are modeled in the event trees. For certain secondary nodes, such as "operator verifies and regulates flow to the steam generator", the actions are implicit in the definitions, and failure is modeled in the fault tree.

As noted above, post-initiator response actions were quantified using a Westinghouse implementation of THERP. An underlying assumption impacting the quantification of post-initiator actions is that the implementation of symptom-based procedures and the associated training on those procedures has reduced, or essentially eliminated, the need for diagnosis as described and modeled in THERP. In the Kewaunee HRA, diagnosis actions in general are modeled as errors of omission and/or commission in performing routine proceduralized actions. The THERP basic HEPs (BHEPs) for "failure to respond to alarms" is used as the probability for error and in many cases, where there is time available, is reduced by a factor of 10 to take further credit for the fact that there are multiple crew members. We recognize that symptom-based procedures and associated training were intended to, and probably have, increased the expected reliability of operator performance in response to accident events.

Unfortunately, there is no systematic study providing firm quantitative evidence of the degree of improvement realized. (A recent study supported by NRC provides some empirical evidence that cognitive tasks such as situation assessment and response planning continue to be important for successful operator response to accident situations.) Most PRAs, including the majority of IPEs we have reviewed to date, still treat the diagnosis, detection, decision making actions following the onset of an accident event as involving a higher level of "cognitive" activity, and therefore use different models/data to quantify those actions. In general, human error probabilities (HEPs) for these actions are lower in the Kewaunee analysis than typical in other studies.

Specific assumptions made by the licensee which in our view contribute to overly optimistic HEPs and/or were applied somewhat "mechanistically" by the licensee without supporting case-by-case assessment include the following:

1) In some cases, a multiplying factor of 0.1 was applied to failure of the crew to diagnose the event by not responding to the appropriate alarm(s), due to "the assumed operating crew experience." This obviously is a speculative modeling assumption in a non-conservative direction, though it is not unreasonable that in some cases where justified by specific analysis, the nominal HEP should be adjusted downward where crews are highly experienced and well-trained, and the alarm response event is annunciated by a particularly compelling and clear annunciation. As discussed above, we believe that the modeling of diagnosis actions in the Kewaunee HRA is already non-conservative. Additional reduction for experienced crews is not justified.

2) Errors of commission are assumed to be less than nominal due to "operating experience and labeling of equipment and controls." A multiplying factor of 0.1 is applied, apparently, to <u>all</u> errors of commission; sometimes even in cases for which the licensee has noted that there may by conditions which would enhance the likelihood of error. This blanket application of additional credit for operating experience and credit for better than nominal labeling of equipment and controls, without case-by-case examination and justification, is in our view an unwarranted non-conservative practice.

3) A multiplying factor of 1, 2, or 5, is applied to account for "low", "moderate", or "high" levels of stress. These values correspond to THERP guidance for "Optimum", "Moderately High", and "Extremely High" stress levels for ***step-by-step*** actions. The THERP values for dynamic tasks are multipliers of 1 and 5 for optimum and moderately high stress, respectively, and a total HEP of 0.25 for extremely high stress. The licensee's use of the values for "step-by-step" tasks for all actions is consistent with the licensee's underlying assumption about the nature of crew response using the symptom-based procedures, but is not consistent with the more typical assumption of treating post-initiator response, especially in diagnosis, detection, decision-making tasks, as dynamic.

4) A nominal HEP of 8.1E-02 is assumed (and applied as a multiplying factor on the basic HEP) for unproceduralized checking, i.e., for the operator to recover his/her own error. The licensee's basis for this value is that operator self-checking during an accident response can be treated as "special short-term, one-of-a-kind checking with alert factors (Table 20-22 in the THERP Handbook, median HEP = 0.05). However, THERP Handbook guidance directs use of this tabulated value only for normal operating conditions. Credit for unproceduralized checking during an accident situation, particularly without specific annunciation or procedures, should be applied very cautiously. The licensee's response to NRC questions indicates that the use of this value is appropriate because it is multiplied by a stress factor. The stress factor does add a degree of conservatism. In our view, however, it does not justify inappropriate application of the THERP tables. In our view blanket application of this recovery factor for unproceduralized checking is non-conservative.

5) Additional credit is taken for recovery of control room operator errors by the STA. A multiplier of 0.1 is applied to the HEP of 8.2E-02 discussed above for unproceduralized checking. The value of 0.1 is obtained by assuming low dependency between the STA and the crew members, and applying the dependency model of THERP (Table 20-17 in the Handbook) as follows:

$$P = (1+19N)/20$$

where N = 8E-01, the HEP for unproceduralized checking

or P = 0.127, rounded off to 0.1

The licensee states that the basis for this credit is the general observation of crew response in the simulator using symptom based procedures and the associated use of safety function status trees by the STA. It does not appear that STA response was evaluated on a case-by-case basis. Review of the sample calculations provided by the licensee in response to NRC's request for additional information indicates that this additional credit for the STA was applied in all cases in which credit was taken for unproceduralized checking (12 out of 12 examples). Some credit for actions by the STA to identify errors in gross actions of the crew is reasonable, providing case-by-case analysis of the accident sequence reveals that the credit is appropriate; e.g., the information provided to the STA through the status trees, annunciators, etc. would clearly identify the error to the STA, that sufficient time existed for recovery of the error after discovery by the STA, etc. A particular concern is the "level" of the operator action to which the STA recovery credit is applied. Obviously, the STA does not act as a "step-by-step" or "over-the-shoulder" checker on detailed actions by each control room crew member. Credit for STA recovery should be considered only for more "global" actions, the tracking of which would be consistent with the STA's role.

The NRC request to the licensee raised an additional question as to whether the assumption of low dependency is applicable for all cases, or reasonably conservative to represent all cases. The licensee assumes that the STA is more than likely not in the control room when the event occurs, or a least is not actively involved in the normal operations, that the STA will arrive in the control room within 10 minutes, and therefore will provide a relatively independent assessment of conditions. This may be the most likely situation. However, in some cases, the STA may be in the room when the event occurs, and STA's actions (at least initially) may be highly dependent on the crew actions. The licensee's assumptions are less conservative than THERP, which assumes low to moderate dependence for the dependency for the first 15 minutes for diagnosis and major events, and high to complete dependency for detailed actions. The licensee's response did not address this issue directly, other than to state that low dependency was assumed.

The credit taken for recovery by the STA is not supported by rigorous assessment (as far as it is possible for us to determine from the document-only review). Blanket application of this additional recovery factor inhibits the ability of the analysts to obtain event-specific insights, and may have resulted in unwarranted non-conservatism, particularly since the multiplying factor is applied to an error probability which appears to be already non-conservative (i.e., unproceduralized checking by the operator on the operator's own performance).

6) A "slack time model" was applied which in some case provides additional credit for recovery by unproceduralized or proceduralized checking. When the slack time, i.e., the difference between the time window available for action and the time required for action, is between 60 minutes and 3 hours, an additional recovery factor (multiplier) of 0.21 is applied to the HEP. The model includes a provision to multiply by an additional factor of 0.54 if the slack time is greater than 3 hours. However, it appears that this provision was not used in the Kewaunee HRA. These recovery factor values are based on the assumed basic error probability for recovery action adjusted to account for dependency (moderate dependency for 60 minutes to 3 hours; high dependency for greater than 3 hours). The unproceduralized checking multiplier of 0.1 noted above is applied for cases in which the slack time is 5 minutes to 60 minutes. Thus, for a slack time of 60 minutes or more, it was assumed that errors made by operators would be recovered, with the probability of failure of the recovery action estimated as a product of (8.0E-02) x (0.1) x (0.21) x [stress factor and other possible factors]. This slack time model is speculative. To our knowledge, it is unique to the Westinghouse implementation of THERP. There is little or no published technical basis for the model. In our view, it is not unreasonable to assume some level of additional credit for recovery of errors when the time available is substantially greater than the time required. However, the credit should be substantiated by a situation-specific assessment. Blanket application of a highly speculative "model", particularly when individnal factors are multiplied, in our view does not lead to a realistic understanding of the human performance involved.

Three types of dependencies in post-initiator human actions were discussed in the submittal: 1) dependencies in manipulating two or more components by the same operator in the same procedure (within-person dependencies, for example, in response to a significant step in an EOP); 2) dependencies between subtasks (actions in response to different EOP steps); and, 3) dependencies between different events (different top-level actions in the same accident sequence, possibly in different procedures).

In cases involving failure to operate two of two controls, the licensee applied the THERP value of 0.15 representing moderate dependency. For actions where the operator manipulates both controls together complete dependency was assumed. Where failure to operate three of three controls was modeled, the second actions has a low dependency of the first, and the third actions has a moderate dependency on the previous actions. For N of N controls (N > or = 4) the fourth and subsequent actions each have a high dependency on previous actions. In cases of M of N controls (2 < M < N), the above dependency level based on the value of M was multiplied by the binomial coefficient of "M".

This model of "within-person" dependency is a reasonable framework for quantifying the subjective judgements involved in assessing dependencies. As with other dependency models, the quantitative value incorporated into the model depends on the judgement of the analyst in assessing the context of the situation in order to arrive at an assumed level of dependency. It is difficult to judge from the document-only review the level of rigor in the licensee's assessment. Based on our review, it appears that the model was applied in a relatively "mechanistic" fashion. That is, there was limited consideration of the factors affecting dependency on a case-by-case basis.

The submittal stated (page 330) that, "In general, zero dependency is assumed between subtasks." The basis provided in the submittal for this assumption was that operators are following the symptom-based procedures on a step-by-step basis ("rule-based" actions), and that dependency would be applicable only if procedural guidance is unavailable or during "knowledge-based" responses. In response to an NRC question, the licensee clarified that this statement referred only to those subtasks which, if failed, cause the entire task to fail. The licensee's response stated that if two or more tasks are "redundant", i.e., more than one subtask has to fail for the task to fail, then the model of dependency described above for within-person dependency in manipulating multiple components was applied. This framework for treating dependencies is analogous to THERP's (or ASEP's) consideration of dependency for series vs. parallel systems, and is reasonable. As discussed above, the effectiveness of this subjective approach depends heavily on the degree of rigor in the analyst's assessment of the factors influencing behavioral dependency, which is difficult to judge from this "document-only" review.

The third type of dependency - between different events - is probably the most significant in terms of the potential for quantitative impact on the estimated CDF. The approach used by the licensee to evaluate these dependencies included application of a decision tree to aid the analyst in determining the level of dependency to be assumed in applying the THERP

dependency model. The decision tree, which was presented in the submittal, considered stress level, the time window for the second task, the amount of slack time, the complexity of the second task, and the type of procedural guidance (essentially quality or clarity of the procedures). While the results still depend on the rigor of the analysis supporting the analyst's judgment, the decision tree provides a systematic framework for the judgement process on a case-by-case basis, and appears to be a reasonable approach.

Vulnerabilities, Insights, and Enhancements

The licensee defines vulnerability as "a feature in plant design, procedures, training, etc., which results in a contribution to core melt risk greater than what is expected." Screening for a vulnerability followed the guidance provided in Appendix 2 to Generic Letter 88-20. Nine vulnerabilities were identified in the submittal, including some related to human-performance issues, such as procedure inadequacies.

Those vulnerabilities identified by the licensee which involve human-performance related issues are:

1) A procedural inadequacy was identified for the Interfacing System LOCA (ISL) event. The most limiting ISL scenario involves a failure of the RHR pump suction valves. When modeling this sequence, it was determined that the procedural guidance in ECA 1.2 for determining the location of LOCA was not complete. WPSC made no effort to assess the impact of each vulnerability on CDF. The response to a request for additional clarification shows the impact of operator error on CDF as negligible (i.e., an increase from 6.63E-05/yr to 6.64E-05/yr), more importantly however is the impact on Level 2 analysis where a guaranteed operator failure would increase containment bypass frequency 1.8%.

2) A major flooding event from the failure of a circulating water expansion joint at the main condenser was identified in the internal flooding analysis. It was determined in the evaluation that routine inspections that could accurately assess the material condition of these expansion joints were not conducted.

3) During assessment of the loss of offsite power (LSP) event it was determined that the instrument air system is not a reliable as it could be. Three of six air compressors are lost as a result of the initiating event making the remaining three very important. Two of the remaining compressors are powered off vital motor control centers (MCC-52A and MCC-62A) with the third receiving its power from a swing-bus (MCC-5262) which is normally aligned to bus 52 and must be manually aligned by the operator to bus 62 if power is lost to bus 52. Procedures for LSP and SBO do not contain guidance for maintainmg MCC-5262 energized. The licensee states in response to NRC's request for additional information that since IPE submittal procedure FR-H.1, Response to Loss of Secondary Heat Sink, has been revised. The HEP calculated value for this action has been determined to be 2.11E-01. This action was not

credited in the IPE submittal model. The licensee's response to NRC's questions indicated that, had this action been included in the IPE, the result would have been a decrease in CDF from 6.6E-05/yr to 6.5E-05/yr (1.3% decrease).

4) During development of the AFW system fault trees, it was determined that a failure of condensate makeup valve (MU-3A) from either loss of control power or instrument air would divert condensate from the condensate storage tanks to the main condenser, and thereby reduce the quantity available to the AFW pumps for secondary cooling. Failure of the operator to isolate this line adversely effects the success of AFW in providing secondary heat removal. In response to follow-up questions, the licensee states that the WPSC staff review of design for the current fail safe position of MU-3A has been completed and no change is planned. In the analysis it was determined that the operators have well over one hour to perform this task and numerous cues are available to alert the operator that the condensate storage tank is emptying.

Important Operator Actions - The submittal does not contain importance calculations for basic events, so additional information was requested from WPSC to identify which of the operator actions are considered most important. The following operator errors were identified as important to CDF by the licensee in response to this request:

Power bus 52 from TSC diesel generator
Cool down and depressurize due to SGTR
Stop RHR pumps when running on miniflow
Cool down and depressurize RCS with SG safeties stuck open
Stop RXCPs due to loss of heat sink
Isolate makeup valve to prevent draining of CST
Establish containment sump recirculation
Align MCC5262 to bus 62
Establish charging in a station blackout

The licensee performed three sensitivity studies related to HRA:

1) All operator actions considered successful,
2) All operator actions increased/decreased by a factor of five, and
3) Identification of Recovery Actions which drop CDF below reporting criteria

Where all operator actions are successful, the results shows an improvement in total core damage frequency of 25% (4.93E-05/year). The licensee notes that are some sequences very sensitive to human reliability failure rates but does not discuss any sequence-specific insights for this case. The licensee cites extensive training on symptom-based procedures and overall operating philosophy with the use of these procedures as the primary reason for such a relatively small impact of removing all operator error.

In the case where all operator action failure rates were increased by a factor or five, the total

core melt frequency increased by a factor of three (1.98E-04). The analysis had the greatest effect on transients with main feedwater and loss of instrument air whose core melt frequency increased by factors of 3.91 and 4.64 respectively. Decreasing human error by a factor of five produced nearly the same results as the case where all actions were successful.

In the assessment of sequences which drop below the core damage frequency criteria because the frequency has been reduced by more than an order of magnitude by credit taken for human recovery actions, the licensee first defined "recovery actions" as:

> "...those actions that the operators perform as a result of a system or component not performing as expected in response to plant emergency conditions. Generally recovery actions are performed outside of the control room. However, if a control room action is unproceduralized or is not a relatively easy task or cannot be completed in a short time it would also be considered a recovery action. Also actions explicitly addressed in the EOPs are not considered recovery actions (e.g. ATWS, MFW after SFW fails and SI recirculation)."

All operator actions modeled in the PRA were screened to identify recovery actions. The screening process identified the following recovery actions:

- Start charging pump powered by TSC diesel (CHB)
- Cool down the RCS during a station blackout (OCD)
- Isolate RHR pumps (OIP)
- Locally establish main feedwater (OM3)
- Locally open SW-1300A or SW-1300B (31-LO-SW1300-HE)
- Align TSC diesel to bus 52 (40--BUS52----HE)

The probability for each recovery action was increased by an order of magnitude and a complete core melt quantification that included a requantification of all fault trees was performed. Three actions are associated with SBO sequences and these accounted for and increase in core melt frequency from 2.64E-05 to 3.37E-05. Two SBO sequences moved above the reporting criteria limit. The two sequences identified include; 1) SBO where RCS cool down fails (OCD) and power not restored in 9 hours, 2) SBO where offsite power is restored (OSP) but charging for seal injection fails (CHB), RCS cooldown fails (OCD) and core is uncovered by RXCP seal LOCA.

The submittal listed two human error related enhancements dealing with procedures changes. In response to NRC's request for additional information, the licensee indicates that these changes have been completed. The first dealt with interfacing systems LOCA (ISL) initiating event. A procedural inadequacy was identified with guidance provided to the operator for determining the location of ISL sequence involving RHR pump isolation valves (most limiting ease). As a result, a procedure ECA 1.2 was changed to provides better guidance for determining leak location for Interfacing system LOCAs. The second enhancement deals with a loss of offsite power (LSP) and a station blackout (SBO). Improved reliability of the

instrument air system was determined possible if additional procedural guidance was given to the operators for local manual switching of MCC-5262 to bus 62 if bus 52 is unavailable. During a LSP/SBO incident three of six air compressors are lost, and of the remaining three compressors, one each receives power from bus 52 and bus 62, with the remaining compressor being normally powered from bus 52 through a swing motor control center. Adding procedural guidance in the case that bus 52 is unavailable will insure at least two air compressors will have power available. In the licensee response to NRC's request for additional information, the licensee notes that procedure changes have been made to provide the necessary guidance. The HEP calculated value for this action has been determined to be 2.11E-01. The licensee also states in their response that, had this action been included in the IPE, the result would have been a decrease in CDF from 6.6E-05/yr to 6.5E-05/yr (1.3% decrease).

In addition to those cited above, two other possible human error enhancements were identified which were under review at the time the submittal was issued, and final determination of applicability of enhancements had not been made. These additional actions were:

- Valve MU-3A, normal makeup from the condensate storage tank to the condenser hotwell, currently fails open on loss of instrument air and/or control power. The emergency makeup valve, MU-3B, fails closed in both cases and this also appears to be the preferred position for MU-3A. In response to follow-up questions, the licensee states that the WPSC staff review of design for the current fail safe position of MU-3A has been completed and As discussed under vulnerabilities above, no change is planned. Further analysis has shown that the operators have well over one hour to perform this task and numerous cues are available to alert the operator that the condensate storage tank is emptying. Based on the results of the revised model iinportance of this operator action has decreased from first to sixth in order of F-V importance.

- In the Level 2 analysis the bypass frequency of 5.28E-06 is dominated by steam generator tube ruptures. The submittal states that these cases are consistent with industry experience and easily remedied with procedural enhancements to refill the RWST and maintain water to the secondary of the ruptured steam generator. The submittal also states that these types of enhancements will be considered in the Kewaunee severe accident management program.

2.0 CONTRACTOR REVIEW FINDINGS

This Technical Evaluation Report (TER) is a summary of the technical review of the human reliability analysis (HRA) presented as part of the Kewaunee Nuclear Power Plant Individual Plant Examination (IPE) submitted by Wisconsin Public Service Corporation (WPSC) to the U.S. Nuclear Regulatory Commission. The review was performed to assist NRC staff in their evaluation of the IPE and conclusion regarding whether the submittal meets the intent of Generic Letter 88-20. The review consisted of a "document-only" review of the submittal and supporting material provided by the WPSC in response to NRC requests for additional information.

2.1 General Review

The licensee's HRA approach addressed primarily post-initiator actions, including response-type and recovery-type actions. A limited-scope assessment of pre-initiator human errors was also included. The analysis of post-initiator actions employed a Westinghouse methodology based on the Technique for Human Error Rate Prediction (THERP) described in NUREG/CR-1278 to quantify human error probabilities (HEPs) for selected operator actions identified from the Emergency Operating procedures (EOPs), System Operating Instructions (SOIs), and Abnormal Operating Procedures (AOPs). The licensee's approach incorporates several underlying assumptions regarding improvements to procedures, training, control room human-machine interface, etc., since the development of THERP which the licensee contends require/permit use of less conservative (lower) error probabilities than provided in the THERP Handbook. While the "realism" or "conservatism" of these assumptions may be arguable, it is important that the licensee's analysis carefully assesses, on a case-by-case basis, the validity of the assumptions and the credit taken for human action, and that the licensee document the basis for these assumptions/credit. The degree to which the licensee performed such an in-depth assessment is difficult to judge in a document-only review, i.e, without a plant visit and more detailed review of tier-2 documentation. However, the impression gained from our review of the submittal and licensee responses to NRC questions is that the licensee may have applied a number of non-conservative assumptions "across the board", without plant-specific and situation-specific evaluation.

2.1.1 Utility Participation and Process for Confirming As-Built, As-Operated Plant.

The utility staff were involved in the development of the IPE. Three Kewaunee staff members were assigned to the IPE development team. All three had previous plant operations experience; two had been Shift Technical Advisers (STAs), and one had been a Senior Reactor Operator (SRO) and Shift Supervisor (SS). A Kewaunee group supervisor served as project manager. Westinghouse personnel provided HRA training to WPSC staff, who then performed the HRA. The submittal states that there was support from other departments in the utility nuclear organization, but does not provide specifics of the areas of expertise or roles of the different participants. The submittal states that because of this involvement, in particular the active involvement of the two STAs through most of the

project, that formal systems walkdowns were not necessary. In response to an NRC request for additional information, the licensee indicated that in the event of any doubt on the part of the STAs, an informal walkdown was performed on the system or system part in question. Further, the licensee noted that detailed walkdowns were performed for internal flooding and Level 2 analyses, and that SROs from Operations and Training reviewed fault trees and system notebooks to assure they represented the as-built configuration. The licensee indicated that plant modifications, Technical Specifications and procedural changes up to the submittal date of 12/1/92 were reflected in the IPE model, with some exceptions related to failure/unavailability data with an end date of December, 1989. The direct involvement of operations staff, combined with informal walkdowns and document review appears to have comprised a reasonable process for assuring that the plant represents the as-built, as-operated plant.

2.1.2 In-House Peer Review.

The licensee conducted an internal review of the IPE. The review team was composed of nine members from Operations, Plant Engineering, Maintenance, and Training Departments, all with plant operations experience. Five of the members were licensed SROs; four were STAs. The review process resulted in more than 450 separate comments. Some technical comments resulted in procedures modifications; others resulted in insights deferred until implementation of the planned accident management program. In addition to this internal staff review, an independent review was provided by contract personnel from Battelle, Safety Management, Inc., Sargent & Lundy, and Wisconsin Electric. Areas of expertise on the external review team included Level 1 PRA, Level 2 PRA, and HRA. The review addressed methodology and overall project quality. The submittal states that in-depth review was provided in areas (including HRA) in which in-house expertise was limited. No specific review comments regarding the HRA review were provided. The combined internal and external review process provided additional assurance of the technical accuracy of the IPE model.

2.2 Pre-Initiator Human Actions

Errors in performance of pre-initiator actions (i.e., actions performed during routine operations and maintenance, 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. The NRC staff review 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.

The Kewaunee HRA included only a very limited-scope assessment of pre-initiator human actions, i.e., human actions during maintenance, test or calibration that could disable a

system. There was no discussion provided in the submittal of a pre-initiator analysis, though two pre-initiator actions were quantified. In response to an NRC request for additional information, the licensee indicated that pre-initiators had been considered qualitatively and generally, and with a few exceptions, had been dismissed from further consideration or quantification. Regarding operator actions to restore equipment after test or maintenance, the licensee states that, "In most cases, the failure of these steps would result in either an annunciator or a status light in the control room to light, alerting the control room operator to such a condition. Shift changes every 12 hours would also have a high probability of detecting such an error. Therefore, these errors are not considered in the HRA." Calibration errors were dismissed without plant-specific assessment because, "They have seldom been shown to be important in past PSAs." The only pre-initiator actions assessed were restoration of manual valves that are used to disable a system's safeguard function during test and maintenance. The licensee's response indicates that all such valve restorations were modeled; none were screened out. However, as indicated above, our review identified only two pre-initiators quantified.

Pre-initiator actions, including miscalibration, have been identified as important contributors in some PRAs, and should not be dismissed without careful, plant-specific, assessment. Lack of a thorough assessment of pre-initiator human errors could result in missing important insights and in overly optimistic estimates of CDF.

2.3 Post-Initiator Human Actions

Errors in post-initiator human actions, e.g., 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. The NRC staff 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.

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 Kewaunee HRA addressed both types of post-initiator human actions.

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

The primary thrust of the NRC staff 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 operating procedures, system instructions, off-normal (or abnormal) event 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.

Identification and selection of operator actions to be quantified in the Kewaunee HRA was based on a review of procedures. The process was not well described in the submittal, but in response to an NRC request for additional information, the licensee provided summary information that indicated a reasonably thorough review process was employed. An initial review was performed by a WPSC HRA analyst (an engineer with STA training), a Westinghouse HRA specialist, and a WPSC SRO. Subsequently, the HRA notebook was reviewed by at least one SRO as part of the internal review process described above. The reviews consisted of analyzing each procedure step in terms of the success criterion for a given fault tree. Only those steps that, if failed, would cause the success criterion not to be met, were considered. Recovery actions were modeled only if they had a major impact on the plant CDF (i.e., more than about 10%), and only if there were symptom-based procedures in place or planned to direct the operators to the required action.

The submittal indicates that since the procedures are based on symptomatic responses, they reduce the diagnosis of an event to responding to cues, thus avoiding the cognitive aspects (diagnosis and decision), concluding that " ...it is advisable not to use Table 20-3 of the THERP handbook," which identifies HEPs for diagnosis by control room personnel of annunciated abnormal events. In response to an NRC request for additional information, the licensee supports this approach based on the inherent nature of symptom-based procedures to minimize cognitive errors and the operators training on these procedures. The effectiveness of diagnosis and decision through the EOPs was assessed through simulator exercises. The simulator exercise observations promote an assumption that EOP actions are not based on available time window pressures.

Actions modeled are generally consistent with actions modeled in other PWR PRAs.

2.3.3 Screening Process for Post-Initiator Human Actions.

No numerical screening process was employed to identify more critical actions and eliminate less important ones from further consideration. All actions identified were quantified and included in the IPE model. Human actions are identified at the functional level through proceduralized tasks tied to the particular accident sequence being considered. These actions are modeled in the event trees. For certain secondary nodes, such as "operator verifies and regulates flow to the steam generator", the actions are implicit in the definitions and failure is modeled in the fault tree.

2.3.4 Quantification of Post-Initiator Human Actions.

The Westinghouse implementation of THERP models each operator actions as consisting of three phases:

1) Cognitive phase (detection/diagnosis/decision to act)

2) Action phase

3) Recovery phase (when the action phase fails).

The probability of failure and the probability of recovery are estimated for the cognitive phase and the action phase, and these four probabilities are combined to derive the overall HEP as follows:

$$Q = Qd*Qdr + Qd*[1-Qd]*Qa*Qar + [1-Qd]*Qa*Qar$$

where Q = HEP estimate
Qd = failure probability in the diagnostic phase
Qdr = failure probability of recovery during the diagnostic phase
Qa = failure probability of action phase
Qar = failure probability of recovery during the action phase.

In most cases, 1-Qd is approximately equal to 1, and [1-Qdr]*Qd is negligibly small. Therefore the equation simplifles to:

$$Q = Qd*Qdr + Qa*Qar$$

This conceptual approach, in which each post-initiator action is treated as consisting of a "cognitive" phase and an "action" phase for which probabilities of failure can be estimated separately and then combined probabilistically to obtain the overall HEP, is consistent with current HRA approaches used in other PRAs. However, in most PRAs, the error probability in the cognitive portion is a significant, often dominant, contributor to the overall HEP. For the Kewaunee HRA, the cognitive portion usually is relatively small or negligible. The licensee expresses in the submittal a fundamental assumption that because of the use of symptom-based procedures and the fact that operators are well trained, the likelihood of error in the cognitive phase is very low or negligible. The result of this basic assumption, plus additional assumptions regarding recovery of error that we believe to be optimistic and not fully justified by the licensee, is that the overall HEPs for post-initiator actions in the Kewaunee IPE are generally lower than typically estimated in other accepted PRAs (e.g., NUREG-1150 studies) and other IPEs.

In our view, the position taken by the licensee regarding diagnosis, or more generally, "cognitive actions" by operators using symptom-based procedures is overly optimistic.

Unfortunately, there is no comprehensive study or empirical data base to substantiate either view. A recently published study supported by NRC (Reference 2) provides some empirical support for our viewpoint that cognitive tasks are still important for successful oprator response to accident situations, even though symptom-based procedures are employed. While the licensee's position may be arguable, it is incumbent upon the licensee to provide a substantive technical basis for application of speculative models, particularly when they are not consistent with most HRA approaches. And, it is important that the validity of the assumptions be assessed on a plant-specific, and to some degree case-by-case, basis. It appears to us, from the document only review, that the licensee frequently made "blanket" assumptions that were applied without substantial evaluation of the specific factors influencing human behavior.

Specific assumptions made by the licensee which in our view contribute to overly optimistic HEPs and/or which were applied somewhat "mechanistically" without detailed analysis include the following:

1) In some cases, a multiplying factor of 0.1 was applied to failure of the crew to diagnose the event by not responding to the appropriate alarm(s), due to "the assumed operating crew experience." This obviously is a speculative modeling assumption in a non-conservative direction, though it is not unreasonable that in some cases where justified by specific analysis, the nominal HEP should be adjusted downward where crews are highly experienced and well-trained, and the alarm response event is annunciated by a particularly compelling and clear annunciation. As discussed above, we believe that the modeling of diagnosis actions in the Kewaunee HRA is already non-conservative. Additional reduction for experienced crews is not justified.

2) Errors of commission are assumed to be less than nominal due to "operating experience and labeling of equipment and controls." A multiplying factor of 0.1 is applied, apparently, to all errors of commission; sometimes even in cases for which the licensee has noted that there may by conditions which would enhance the likelihood of error. This blanket application of additional credit for operating experience and credit for better than nominal labeling of equipment and controls, without case-by-case examination and justification, is in our view an unwarranted non-conservative practice.

3) A multiplying factor of 1, 2, or 5, is applied to account for "low", "moderate", or "high" levels of stress. These values correspond to THERP guidance for "Optimum", "Moderately High", and "Extremely High" stress levels for *step-by-step* actions. The THERP values for dynamic tasks are multipliers of 1 and 5 for optimum and moderately high stress, respectively, and a total HEP of 0.25 for extremely high stress. The licensee's use of the values for "step-by-step" tasks for all actions is consistent with the licensee's underlying assumption about the nature of crew response using the symptom-based procedures, but is not consistent with the more typical assumption of treating post-initiator response, especially in diagnosis, detection,

decision-making tasks, as dynamic.

4) A nominal HEP of 8.1E-02 is assumed (and applied as a multiplying factor on the basic HEP) for unproceduralized checking, i.e., for the operator to recover his/her own error. The licensee's basis for this value is that operator self-checking during an accident response can be treated as "special short-term, one-of-a-kind checking with alert factors (Table 20-22 in the THERP Handbook, median HEP = 0.05). However, THERP Handbook guidance directs use of this tabulated value only for normal operating conditions. Credit for unproceduralized checking during an accident situation, particularly without specific annunciation or procedures, should be applied very cautiously. The licensee's response to NRC questions indicates that the use of this value is appropriate because it is multiplied by a stress factor. The stress factor does add a degree of conservatism. In our view, however, it does not justify inappropriate application of the THERP tables. In our view blanket application of this recovery factor for unprocedurized checking is non-conservative.

5) Additional credit is taken for recovery of control room operator errors by the STA. A multiplier of 0.1 is applied to the HEP of 8.2E-02 discussed above for unproceduralized checking. The value of 0.1 is obtained by assuming low dependency between the STA and the crew members, and applying the dependency model of THERP (Table 20-17 in the Handbook) as follows:

$$P = (1+19N)/20$$

where N = 8E-01, the HEP for unproceduralized checking

or $P = 0.127$, rounded off to 0.1

The licensee states that the basis for this credit is the general observation of crew response in the simulator using symptom based procedures and the associated use of safety function status trees by the STA. It does not appear that STA response was evaluated on a case-by-case basis. Review of the sample calculations provided by the licensee in response to NRC's request for additional information indicates that this additional credit for the STA was applied in all cases in which credit was taken for unproceduralized checking (12 out of 12 examples). Some credit for actions by the STA to identify errors in gross actions of the crew is reasonable, providing case-by-case analysis of the accident sequence revcals that the credit is appropriate; e.g., the information provided to the STA through the status trees, annunciators, etc. would clearly identify the error to the STA, that sufficient time existed for recovery of the error after discovery by the STA, etc. A particular concern is the "level" of the operator action to which the STA recovery credit is applied. Obviously, the STA does not act as a "step-by-step" or "over-the-shoulder" checker on detailed actions by each control room crew member. Credit for STA recovery should be considered only for more "global" actions, the tracking of which would be consistent with the STA's

role.

The NRC request to the licensee raised an additional question as to whether the assumption of low dependency is applicable for all cases, or reasonably conservative to represent all cases. The licensee assumes that the STA is more than likely not in the control room when the event occurs, or a least is not actively involved in the normal operations, that the STA will arrive in the control room within 10 minutes, and therefore will provide a relatively independent assessment of conditions. This may be the most likely situation. However, in some cases, the STA may be in the room when the event occurs, and STA's actions (at least initially) may be highly dependent on the crew actions. The licensee's assumptions are less conservative than THERP, which assumes low to moderate dependence for the dependency for the first 15 minutes for diagnosis and major events, and high to complete dependency for detailed actions. The licensee's response did not address this issue directly, other than to state that low dependency was assumed.

The credit taken for recovery by the STA is not supported by rigorous assessment (as far as it is possible for us to determine from the document-only review). Blanket application of this additional recovery factor inhibits the ability of the analysts to obtain event-specific insights, and may have resulted in unwarranted non-conservatism, particularly since the multiplying factor is applied to an error probability which appears to be already non-conservative (i.e., unproceduralized checking by the operator on the operator's own performance).

6) A "slack time model" was applied which in some case provides additional credit for recovery by unproceduralized or proceduralized checking. When the slack time, i.e., the difference between the time window available for action and the time required for action, is between 60 minutes and 3 hours, an additional recovery factor (multiplier) of 0.21 is applied to the HEP. The model includes a provision to multiply by an additional factor of 0.54 if the slack time is greater than 3 hours. However, it appears that this provision was not used in the Kewaunee HRA. These recovery factor values are based on the assumed basic error probability for recovery action adjusted to account for dependency (moderate dependency for 60 minutes to 3 hours; high dependency for greater than 3 hours). The unproceduralized checking multiplier of 0.1 noted above is applied for cases in which the slack time is 5 minutes to 60 minutes. Thus, for a slack time of 60 minutes or more, it was assumed that errors made by operators would be recovered, with the probability of failure of the recovery action estimated as a product of (8.0E-02) x (0.1) x (0.21) x [stress factor and other possible factors]. This slack time model is speculative. To our knowledge, it is unique to the Westinghouse implementation of THERP. There is little or no published technical basis for the model. In our view, it is not unreasonable to assume some level of additional credit for recovery of errors when the time available is substantially greater than the time required. However, the credit should be substantiated by a situation-specific assessment. Blanket application of a highly speculative "model",

particularly when individual factors are multiplied, in our view does not lead to a realistic understanding of the human performance involved.

Three types of dependencies in post-initiator human actions were discussed in the submittal:

1) Dependencies in manipulating two or more components by the same operator in the same procedure (within-person dependencies, for example, in response to a significant step in an EOP),

2) Dependencies between subtasks (actions in response to different EOP steps); and,

3) Dependencies between different events (different top-level actions in the same accident sequence, possibly in different procedures).

In cases involving failure to operate two of two controls, the licensee applied the THERP value of 0.15 representing moderate dependency. For actions where the operator manipulates both controls together complete dependency was assumed. Where failure to operate three of three controls was modeled, the second actions has a low dependency of the first, and the third actions has a moderate dependency on the previous actions. For N of N controls (N > or = 4) the fourth and subsequent actions each have a high dependency on previous actions. In cases of M of N controls (2 < M < N), the above dependency level based on the value of M was multiplied by the binomial coefficient of "M".

This model of "within-person" dependency is a reasonable framework for quantifying the subjective judgements involved in assessing dependencies. As with other dependency models, the quantitative value incorporated into the model depends on the judgement of the analyst in assessing the context of the situation, in order to arrive at an assumed level of dependency. It is difficult to judge from the document-only review the level of rigor in the licensee's assessment. Based on our review, it appears that the model was applied in a relatively "mechanistic" fashion. That is, there was limited consideration of the factors affecting dependency on a case-by-case basis.

The submittal stated (page 330) that, "In general, zero dependency is assumed between subtasks." The basis provided in the submittal for this assumption was that operators are following the symptom-based procedures on a step-by-step basis ("rule-based" actions), and that dependency would be applicable only if procedural guidance is unavailable or during "knowledge-based" responses. In response to an NRC question, the licensee clarified that this statement referred only to those subtasks which, if failed, cause the entire task to fail. The licensee's response stated that if two or more tasks are "redundant", i.e., more than one subtask has to fail for the task to fail, then the model of dependency described above for within-person dependency in manipulating multiple components was applied. This framework for treating dependencies is analogous to THERP's (or ASEP's) consideration of dependency for series vs. parallel systems, and is reasonable. As discussed above, the effectiveness of this subjective approach depends heavily on the degree of rigor in the analyst's assessment of

the factors influencing behavioral dependency, which is difficult to judge from this "document-only" review.

The third type of dependency - between different events - is probably the most significant in terms of the potential for quantitative impact on the estimated CDF. The approach used by the licensee to evaluate these dependencies included application of a decision tree to aid the analyst in determining the level of dependency to be assumed in applying the THERP dependency model. The decision tree, which was presented in the submittal, considered stress level, the time window for the second task, the amount of slack time, the complexity of the second task, and the type of procedural guidance (essentially quality or clarity of the procedures). While the results still depend on the rigor of the analysis supporting the analyst's judgment, the decision tree provides a systematic framework for the judgement process on a case-by-case basis, and appears to be a reasonable approach.

3.0 VULNERABILITIES, INSIGHTS, AND ENHANCEMENTS

3.1 Vulnerabilities

The licensee defines vulnerability as "a feature in plant design, procedures, training, etc., which results in a contribution to core melt risk greater than what is expected." Screening for a vulnerability followed the guidance provided in Appendix 2 to Generic Letter 88-20. Those criteria selected by Kewaunee for reporting potentially important sequences that might lead to core damage or unusually poor containment performance are as follows:

- Any systemic sequence that contributes 1E-7 or more per reactor year to core damage.
- All systemic sequences within the upper 95 percent of the total core damage frequency.
- All systemic sequences within the upper 95 percent of the total containment failure frequency.
- Systemic sequences that contribute to a containment bypass frequency in excess of 1E-8 per reactor year.
- Any systemic sequences that the utility determines from previous PRAs or by utility engineering judgement to be important contributors to core damage frequency or poor containment performance.
- Identification of sequences that, but for low human error rates in recovery actions, would have been above the applicable core damage screening criteria.

Nine vulnerabilities were identified in the submittal and four of these involve human-performance related issues, namely:

1) A procedural inadequacy was identified for the Interfacing System LOCA (ISL) event. The most limiting ISL scenario involves a failure of the RHR pump suction valves. When modeling this sequence, it was determined that the procedural guidance in ECA 1.2 for determining the location of LOCA was not complete.

   WPSC made no effort to assess the impact of each vulnerability on CDF. In response to a request for additional clarification the licensee implies that analysis shows the impact on CDF as negligible (i.e., an increase from 6.63E-05/yr to 6.64E-05/yr) and the more important impact is on Level 2 analysis where a guaranteed failure would increase containment bypass frequency 1.8%.

2) A major flooding event from the failure of a circulating water expansion joint at the main condenser was identified in the internal flooding analysis. It was determined in the evaluation that routine inspections that could accurately assess the material condition of these expansion joints were not conducted.

3) During assessment of the loss of offsite power (LSP) event it was determined that the instrument air system is not a reliable as it could be. Three of six air compressors are

lost as a result of the initiating event making the remaining three very important. Two of the remaining compressors are powered off vital motor control centers (MCC-52A and MCC-62A) with the third receiving its power from a swing-bus (MCC-5262) which is normally aligned to bus 52 and must be manually aligned by the operator to bus 62 if power is lost to bus 52. Procedures for LSP and SBO do not contain guidance for maintaining MCC-5262 energized. The licensee states in response to NRC's request for additional information that since IPE submittal procedure FR-H.1, Response to Loss of Secondary Heat Sink, has been revised. The HEP calculated value for this action has been determined to be 2.11E-01. This action was not credited in the IPE submittal model. The licensee's response to NRC's questions indicated that, had this action been included in the IPE, the result would have been a decrease in CDF from 6.6E-05/yr to 6.5E-05/yr (1.3% decrease).

4) During development of the AFW system fault trees it was determined that a failure of condensate makeup valve (MU-3A) from either loss of control power or instrument air would divert condensate from the condensate storage tanks to the main condenser, and thereby reduce the quantity available to the AFW pumps for secondary cooling. Failure of the operator to isolate this line adversely effects the success of AFW in providing secondary heat removal.

   In response to follow-up questions, the licensee states that the WPSC staff review of design for the current fail safe position of MU-3A has been completed and no change is planned. Further analysis has shown that the operators have well over one hour to perform this task and numerous cues are available to alert the operator that the condensate storage tank is emptying.

3.2 Insights

The submittal does not contain importance calculations for basic events, so additional information was requested to identify which of the operator actions are considered most important. The information contained in Table 3-1, is reproduced from the answer provided by the licensee in response to this request.

Table 3-1, Most Important Human Actions (Fussel-Vesely importance > 0.2%)

DESCRIPTION	HEP	SUBMITTAL MODEL IMPORTANCE	REVISED MODEL IMPORTANCE
Isolate makeup valve to prevent draining of CST (05BAV-MU-3A---HE)	7.68E-02	9.3%	1.9%
Cool down and depressurize due to SGTR (OSI)	9.8E-03	6.0%	5.6%
Stop RHR pumps when running on miniflow (34I---L12A---HE)	4.23E-04	4.9%	4.7%

Cool down and depressurize RCS with SG safeties stuck open (EC4)	5.00E-02	4.7%	4.4%
Stop RXCPs due to loss of heat sink (36-RXCP-STOP-HE)	2.33E-03	3.5%	3.3%
Establish charging in a station blackout (CHB)	1.00E-02	0.6%	0.2%
Power bus 52 from TSC diesel generator (40-BUS52---HE)	1.00E-02	0.6%	17.5%
Establish containment sump recirculation (33R-2TRN-REC-HE)	4.92E-05	0.4%	0.4%
Align MCC5262 to bus 62 (40-MCC5262-HE)	2.11E-01	N/A	0.3%

NOTE: The importance values in this table are results provided by the licensee in response to an NRC request for additional information. They are based on revised calculations completed after submittal of the IPE.

The ranking for the operator action to Isolate makeup valve to prevent draining of CST (05BAV-MU-3A---HE) dropped from first to sixth following reassessment which identified cues available to alert the operator and additional time available for accomplishment. The licensee's discussion of the assessment leading to this revised importance does not identify any considerations given to possible improvements to operator training or procedural guidance.

The licensee performed three sensitivity studies related to HRA. These studies include:

- All operator actions successful
- All operator actions increased/decreased by a factor of five
- Identification of Recovery Actions which drop CDF below reporting criteria

Where all operator actions are successful, the results shows an improvement in total core damage frequency of 25% (4.93E-05/year). The licensee notes that are some sequences very sensitive to human reliability failure rates but does not discuss any sequence-specific insights for this case. The licensee cites extensive training on symptom-based procedures and overall operating philosophy with the use of these procedures as the primary reason for such a relatively small impact of removing all operator error.

In the case where all operator action failure rates were increased by a factor or five, the total core melt frequency increased by a factor of three (1.98E-04). The analysis had the greatest effect on transients with main feedwater and loss of instrument air whose core melt frequency increased by factors of 3.91 and 4.64 respectively. Decreasing human error by a factor of five produced nearly the same results as the case where all actions were successful.

In the assessment of sequences which drop below the core damage frequency criteria because the frequency has been reduced by more than an order of magnitude by credit taken for human recovery actions, the licensee first defined "recovery actions" as:

> "...those actions that the operators perform as a result of a system or component not performing as expected in response to plant emergency conditions. Generally recovery actions are performed outside of the control room. However, if a control room action is unproceduralized or is not a relatively easy task or cannot be completed in a short time it would also be considered a recovery action. Also actions explicitly addressed in the EOPs are not considered recovery actions (e.g. ATWS, MFW after SFW fails and SI recirculation)."

Screening of all operator actions modeled in the PRA generated the list of actions shown in Table 3-2.

The probability for each recovery action was increased by an order of magnitude and a complete core melt quantification that included a requantification of all fault trees was performed. As seen in Table 3-2 below, three actions are associated with SBO sequences and these accounted for and increase in core melt frequency from 2.64E-05 to 3.37E-05. Two SBO sequences moved above the reporting criteria limit. The two sequences identified include; 1) SBO where RCS cool down fails (OCD) and power not restored in 9 hours, 2) SBO where offsite power is restored but charging for seal injection fails, RCS cooldown fails and core is uncovered by RXCP seal LOCA.

Table 3-2, Recovery Actions

Description	Event Identifier
Start charging pump powered by TSC diesel	CHB
Cool down the RCS during a station blackout	OCD
Isolate RHR pumps	OIP
Locally establish main feedwater	OM3
Locally open SW-1300A or SW-1300B	31-LO-SW1300-HE
Align TSC diesel to bus 52	40--BUS52---HE

3.3 Enhancements

Section 6.0 of the submittal addresses specific safety issues and potential improvements. IPE Table 6-1 lists two human error related enhancements dealing with procedures changes. The licensee indicates that these changes have been completed in their response to NRC's request for additional information. The first deals with interfacing systems LOCA (ISL) initiating

event. As described in submittal Section 3.4.3.B.2., a procedural inadequacy was identified with guidance provided to the operator for determining the location of ISL sequence involving RHR pump isolation valves (most limiting case). As a result, a procedure ECA 1.2 was changed to provides better guidance for determining leak location for Interfacing system LOCAs. The second enhancement deal with a loss of offsite power (LSP) and a station blackout (SBO). As discussed in Section 3.4.3.B.5., improved reliability of the instrument air system was determined possible if additional procedural guidance was given to the operators for local manual switching of MCC-5262 to bus 62 if bus 52 is unavailable. During a LSP/SBO incident three of six air compressors are lost, and of the remaining three compressors, one each receives power from bus 52 and bus 62, with the remaining compressor being normally powered from bus 52 through a swing motor control center. Adding procedural guidance in the case that bus 52 is unavailable will insure at least two air compressors will have power available. In the licensee response to NRC's request for additional information the licensee notes that procedure changes have been made to provide the necessary guidance. The HEP calculated value for this action has been determined to be 2.11E-01. The licensee also states in their response that, had this action been included in the IPE, the result would have been a decrease in CDF from 6.6E-05/yr to 6.5E-05/yr (1.3% decrcase).

The licensee identified two other possible human error related plant vulnerabilities during their review of the sensitivity and importance analysis which were under evaluation for possible enhancements at the time the submittal was issued. These additional actions are:

- Valve MU-3A, normal makeup from the condensate storage tank to the condenser hotwell, currently fails open on loss of instrument air and/or control power. The emergency makeup valve, MU-3B, fails closed in both cases and this also appears to be the preferred position for MU-3A. In response to follow-up questions, the licensee states that the WPSC staff review of design for the current fail safe position of MU-3A has been completed and As discussed under vulnerabilities above, no change is planned. Further analysis has shown that the operators have well over one hour to perform this task and numerous cues are available to alert the operator that the condensate storage tank is emptying. Based on the results of the revised model importance of this operator action has decreased from first to sixth in order of F-V importance.

- In the Level 2 analysis the bypass frequency of 5.28E-06 is dominated by steam generator tube ruptures. The submittal states that these cases are consistent with industry experience and easily remedied with procedural enhancements to refill the RWST and maintain water to the secondary of the ruptured steam generator. The submittal also states that these types of enhancements will be considered in the Kewaunee severe accident management program.

4.0 OVERALL EVALUATION AND CONCLUSION

In general, we view the licensee's approach to quantification of human performance as optimistic, particularly in the treatment of post-initiator human actions. The quantification methodology employed is the Westinghouse adaptation of THERP, which at a general level follows the THERP guidance. However, the licensee has made a basic assumption that introduction of symptom-based procedures and improved training have essentially eliminated the need for "cognitive" action (diagnosis, detection, decision making) in response to an accident event. Consequently, the licensee's quantification process employs THERP models and attendant assumptions that are appropriate for "step-by-step" actions, and in some cases for normal (pre-initiator) actions, to quantify post-initiator actions. Even when the licensee designates an action as a diagnosis action, the quantification used THERP tables and values that are intended to address simple errors of omission/commission in response to annunciators or procedures. The THERP diagnostic model was felt by the licensee to be inappropriate and was not used. Most HRAs performed to date have viewed post-initiator actions as consisting of both diagnosis/ decision/ detection actions, and execution actions; and most have recognized that actions following an accident event, especially earlier in the accident sequence, are more of a "dynamic" nature than simple step-by-step procedural response. In general, the licensee's detailed HRA modeling assumptions are consistent with this underlying assumption. However, the licensee does not present a substantive technical basis for this basic assumption. A recent NUREG/CR report (Ref. 2) provides some empirical evidence in support of the more "conventional" view that cognitive demands, such as situation assessment and response planning continue to be important for successful operator response to accident situations, even when symptom-based EOPs are employed.

A second general conclusion is that the licensee in a number of instances appears to have applied credit for human error recovery mechanisms that may be unrealistically optimistic. More importantly, credit is sometimes applied in a "mechanistic" fashion using a simplified and speculative model "across the board" without a significant case-by-case assessment to verify that the underlying assumptions of the model are applicable. As we have noted several times previously, the degree of rigor in the plant-specific and case-by-case assessment is difficult to determine from the document-only review. The IPE submittal, in direct compliance with NUREG-1335 guidance, is not intended to provide detailed calculations and associated "Tier 2" information. However, our general impression from the submittal and the licensee's response to NRC questions is that the case-by-case analysis was limited. The depth of insight obtainable from the analysis regarding important contributors to human performance is a function of the rigor and level of depth/detail of the qualitative analysis.

Some of the key specific features/assumptions of the licensee's HRA analysis that help form a basis for these general conclusions are as follows:

1) Blanket use of speculative modeling assumption for crew experience and alarm

cues - A multiplying factor of 0.1 was applied to failure of the crew to diagnose the event by not responding to the appropriate alarm(s), due to "the assumed operating crew experience." This is a speculative modeling assumption in a non-conservative direction, though it is not unreasonable that in some cases where justified by specific analysis, the nominal HEP should be adjusted downward where crews are highly experienced and well-trained, and the alarm response event is annunciated by a particularly compelling and clear annunciation. We believe that the modeling of diagnosis actions in the Kewaunee HRA is already non-conservative. Additional reduction for experienced crews is not justified.

2) Blanket application of credit for operator experience and labeling of equipment and controls - Errors of commission are assumed to be less than nominal due to "operating experience and labeling of equipment and controls." A multiplying factor of 0.1 is applied, apparently, to all errors of commission; sometimes even in cases for which the licensee has noted that there may by conditions which would enhance the likelihood of error. This blanket application of additional credit for operating experience and credit for better than nominal labeling of equipment and controls, without case-by-case examination and justification, is in our view an unwarranted non-conservative practice.

3) Use of "step-by-step" THERP stress values for dynamic tasks applications - A multiplying factor of 1, 2, or 5, is applied to account for "low", "moderate", or "high" levels of stress. These values correspond to THERP guidance for "Optimum", "Moderately High", and "Extremely High" stress levels for ***step-by-step*** actions. The THERP values for dynamic tasks are multipliers of 1 and 5 for optimum and moderately high stress, respectively, and a total HEP of 0.25 for extremely high stress. The licensee's use of the values for "step-by-step" tasks for all actions is consistent with the licensee's underlying assumption about the nature of crew response using the symptom-based procedures, but is not consistent with the more typical assumption of treating post-initiator response, especially in diagnosis, detection, decision-making tasks, as dynamic.

4) Limited consideration of pre-initiator human actions - The Kewaunee HRA included only a limited set of pre-initiator human actions, i.e., human actions during maintenance, test or calibration that could disable a system. In response to an NRC request for additional information, the licensee indicated that pre-initiators had been considered qualitatively and generally, and with a few exceptions, had been dismissed from further consideration or quantification. Regarding operator actions to restore equipment after test or maintenance, the licensee states that, "In most cases, the failure of these steps would result in either an annunciator or a status light in the control room to light, alerting the control room operator to such a condition. Shift changes every 12 hours would also have a high probability of detecting such an error. Therefore, these errors are not considered in the HRA." Calibration errors were dismissed without plant-specific assessment because, "They

have seldom been shown to be important in past PSAs." Pre-initiator actions, including miscalibration, have been identified as important contributors in some PRAs, and should not be dismissed without careful, plant-specific, assessment.

5) Unproceduralized checking by the control room operators - A nominal HEP of 8.1E-02 is assumed (and applied as a multiplying factor on the basic HEP) for unproceduralized checking, i.e., for the operator to recover his own error. The licensee's basis for this value is that operator self-checking during an accident response can be treated as "special short-term, one-of-a-kind checking with alert factors (Table 20-22 in the THERP Handbook, median HEP = 0.05). However, THERP Handbook guidance directs use of this tabulated value only for normal operating conditions. Credit for unproceduralized checking during an accident situation, particularly without specific annunciation or procedures, should be applied very cautiously. The licensee's response to NRC questions indicates that the use of this value is appropriate because it is multiplied by a stress factor. The stress factor does add a degree of conservatism. In our view, however, it does not justify inappropriate application of the THERP tables. In our view blanket application of this recovery factor for unprocedurized checking is non-conservative.

6) Blanket application of credit for STA recovery of operator error - It does not appear that STA response was evaluated on a case-by-case basis. Review of the sample calculations provided by the licensee in response to NRC's request for additional information indicates that this additional credit for the STA was applied in all cases in which credit was taken for unproceduralized checking (12 out of 12 examples). Some credit for actions by the STA to identify errors in gross actions of the crew is reasonable, providing that case-by-case analysis of the accident sequence reveals that the credit is appropriate; e.g., the information provided to the STA through the status trees, annunciators, etc. would clearly identify the error to the STA, that sufficient time existed for recovery of the error after discovery by the STA, etc. A particular concern is the "level" of the operator action to which the STA recovery credit is applied. Obviously, the STA does not act as a "step-by-step" or "over-the-shoulder" checker on detailed actions by each control room crew member. Credit for STA recovery should be considered only for more "global" actions, the tracking of which would be consistent with the STA's role. The credit taken for recovery by the STA is not supported by rigorous assessment (as far as it is possible for us to determine from the document-only review). Blanket application of this additional recovery factor inhibits the ability of the analysts to obtain event-specific insights, and may have resulted in unwarranted non-conservatism, particularly since the multiplying factor is applied to an error probability which appears to be already non-conservative (i.e., unproceduralized checking by the operator on the operator's own performance).

7) Blanket application of the slack-time model - A "slack time model" was applied which in some case provides additional credit for recovery by unproceduralized or proceduralized checking. When the slack time, i.e., the difference between the time window available for action and the time required for action, is between 60 minutes and 3 hours, an additional recovery factor (multiplier) of 0.21 is applied to the HEP. The model includes a provision to multiply by an additional factor of 0.54 if the slack time is greater than 3 hours. However, it appears that this provision was not used in the Kewaunee HRA. These recovery factor values are based on the assumed basic error probability for recovery action adjusted to account for dependency (moderate dependency for 60 minutes to 3 hours; high dependency for greater than 3 hours). The unproceduralized checking multiplier of 0.1 noted above is applied for cases in which the slack time is 5 minutes to 60 minutes. Thus, for a slack time of 60 minutes or more, it was assumed that errors made by operators would be recovered, with the probability of failure of the recovery action estimated as a product of (8.0E-02) x (0.1) x (0.21) x [stress factor and other possible factors]. This slack time model is speculative. To our knowledge, it is unique to the Westinghouse implementation of THERP. There is little or no published technical basis for the model. In our view, it is not unreasonable to assume some level of additional credit for recovery of errors when the time available is substantially greater than the time required. However, the credit should be substantiated by a situation-specific assessment. Blanket application of a highly speculative "model", particularly when individual factors are multiplied, in our view does not lead to a realistic understanding of the human performance involved.

The licensee's treatment of dependencies in post-initiator actions followed the general structure provided by the THERP dependency model (Chapter 10 of the Handbook, summarized in Tables 20-17 and 20-18). The licensee addressed dependency with regard to three types of actions: 1) within-person dependencies in execution of actions involving multiple controls; 2) dependencies in performance of individual subtasks (major steps) within the symptom-based procedures; and, 3) dependencies between two different events (human actions) within the same accident sequences. All three methods are speculative and involve substantial judgement on the part of the analyst (as do all current approaches to quantification of dependency). The licensee's treatment of the first two types appeared to be somewhat "mechanistic," i.e., did not appear to involve significant case-by-case evaluation of the behavioral context of the action and the factors potentially influencing the level of dependency. In the licensee's treatment of the third type of dependency, which probably is the most significant in terms of quantitative impact on the IPE results, subjective judgment was guided by decision tree which appears to have been applied on a case-by-case basis. Overall, the treatment of dependencies by the licensee is reasonable in comparison to treatment in other current PRAs.

The licensee's process for screening of vulnerabilities followed the guidance provided in Appendix 2 to Generic Letter 88-20. Nine vulnerabilities were identified in the

submittal, including some related to human-performance issues, such as procedure inadequacies. The licensee provided a table of important operator actions in response to a NRC question. This table cited results from a revised model which shows a marked change in importance between IPE and revised version results for those operator actions listed.

REFERENCES

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

2. E.M. Roth, R.J. Mumaw, P.M. Lewis, "An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies," NUREG/CR-6208, July, 1994.

KEWAUNEE NUCLEAR POWER PLANT
HUMAN RELIABILITY ANALYSIS
DATA SUMMARY SHEETS

Important Operator Actions/Errors:

Importance evaluations were reported in response to a request for additional information. The events, HEPs, and the Fussel-Vesely importance ranking for those human errors with F-V values greater than 0.2% are as follows:

Operator Action Importance to Core Damage

EVENT DESCRIPTION	HEP	F-V IMPORTANCE (see note)
Power bus 52 from TSC diesel generator (40-BUS52—HE)	1.00E-02	17.5% (0.6%)
Cool down and depressurize due to SGTR (OSI)	9.8E-03	5.6% (6.0%)
Stop RHR pumps when running on miniflow (34I—L12A—HE)	4.23E-04	4.7% (4.9%)
Cool down and depressurize RCS with SG safeties stuck open (EC4)	5.00E-02	4.4% (4.7%)
Stop RXCPs due to loss of heat sink (36-RXCP-STOP-HE)	2.33E-03	3.3% (3.5%)
Isolate makeup valve to prevent draining of CST (05BAV-MU-3A—HE)	7.68E-02	1.9% (9.3%)
Establish containment sump recirculation (33R-2TRN-REC-HE)	4.92E-05	0.4% (0.4%)
Align MCC5262 to bus 62 (40-MCC5262-HE)	2.11E-01	0.3% (N/A)
Establish charging in a station blackout (CHB)	1.00E-02	0.2% (0.6%)

Note: The F-V values are rank ordered as to importance determined when the analysis was rerun with the revised model, the values in parentheses are the rankings which appeared in the submittal.

Human-Performance Related Enhancements:

Four significant human-performance-related enhancements were reported as resulting from the IPE/HRA analysis:

1) A procedural inadequacy was identified for the Interfacing System LOCA (ISL) event. The most limiting ISL scenario involves a failure of the RHR pump suction valves. When modeling this sequence, it was determined that the procedural guidance in ECA 1.2 for determining the location of LOCA was not complete.

2) A major flooding event from the failure of a circulating water expansion joint at the main condenser was identified in the internal flooding analysis. It was determined in the evaluation that routine inspections that could accurately assess the material condition of these expansion joints.

3) During assessment of the loss of offsite power (LSP) event it was determined that the instrument air system is not a reliable as it could be. Three of six air compressors are lost as a result of the initiating event making the remaining three very important. Two of the remaining compressors are powered off vital motor control centers (MCC-52A and MCC-62A) with the third receiving its power from a swing-bus (MCC-5262) which is normally aligned to bus 52 and must be manually aligned by the operator to bus 62 if power is lost to bus 52. Procedures for LSP and SBO do not contain guidance for maintaining MCC-5262 energized. The licensee states in response to NRC's request for additional information that since IPE submittal procedure FR-H.1, Response to Loss of Secondary Heat Sink, has been revised. The HEP calculated value for this action has been determined to be 2.11E-01. This action was not credited in the IPE submittal model. The licensee's response to NRC's questions indicated that, had this action been included in the IPE, the result would have been a decrease in CDF from 6.6E-05/yr to 6.5E-05/yr (1.3% decrease).

4) In the Level 2 analysis the bypass frequency of 5.28E-06 is dominated by steam generator tube ruptures. These cases are consistent with industry experience and easily remedied with procedural enhancements to refill the RWST and maintain water to the secondary of the ruptured steam generator. These types of enhancements will be considered in the Kewaunee severe accident management program.

APPENDIX D

KEWAUNEE NUCLEAR POWER PLANT INDIVIDUAL PLANT EXAMINATION

TECHNICAL EVALUATION REPORT

(REVISED HUMAN RELIABILITY ANALYSIS)

Review of Kewaunee Revised Human Reliability Analysis

1. Introduction

The human reliability analysis performed as part of the Kewaunee IPE was re-performed by the licensee to remove concerns with the HRA method expressed by NRC. The reanalysis was submitted to NRC as two attachments to a letter to NRC dated June 27, 1996, from Mr. C. R. Steinhardt, Senior Vice President - Nuclear Power, Wisconsin Public Service Corporation. This review is performed of the reanalysis.

The principal revision was to change the method used to analyze and quantify the post-initiator human action events. The original Kewaunee HRA modeling was performed using a modified version of THERP, as described in the Technical Evaluation Report associated with the original submittal. This method has been found to lead to shortcomings in HRA models used in some IPEs, particularly because of its lack of consideration of activities associated with decisionmaking, its limited set of human failure mechanisms, the limited number of PSFs considered, and the limited analysis of dependencies between human actions.

In addition, the licensee provided an analysis of very few pre-initiator human actions in the original submittal--the analysis was limited to only two sets of manual valves that are moved during testing to a position that would fail the equipment in the event of an initiating event. Many more pre-initiator human actions were included in the reanalysis.

2. Analysis of Pre-Initiator Human Actions

One limitation of the original Kewaunee IPE was the exclusion of most pre-initiator human actions, including those associated with calibration activities.

In the revised analysis, the licensee analyzed 44 pre-initiator human actions, including three miscalibration errors. The licensee presented no description of the process by which these actions were identified for analysis, other than stating that they were identified by the systems' analysts "as events representing valves or switches in an incorrect configuration." No description of procedural reviews or discussions with personnel involved in maintenance, test, or calibration activities is presented in the submittal.

The licensee first applied a primarily qualitative screening process to remove those pre-initiator actions that have "a very low probability of occurrence" from the detailed evaluation. The following criteria were used in the screening analysis:

- if the reconfigured components are misaligned but not disabled, and they receive a realignment sigual on system demand, then the activity is screened out;

- if the activity is a maintenance activity and a full functional test is carried out on

completion of the maintenance, then the activity is screened out; and

- if the activity reconfigures a component to the safeguard position or is not used during accident mitigation, the activity is screened out.

In addition, if the activity is not screened out based on these qualitative criteria but has a calculated human error probability of 1E-06 or less, the activity is screened out.

The licensee states that the qnantitative analysis of pre-initiator human actions was performed using the simplified THERP HRA method developed for the NRC's Accident Sequence Evaluation Program (ASEP), described in NUREG/CR-4722. In general the calculation process followed the guidelines presented in Chapter 5, ASEP Nominal HRA for Pre-Accident Tasks, of NUREG/CR- 4772. That is, a basic median human error probability of 0.03 per activity was assumed, which was then adjusted for several potential recovery mechanisms. In the case of Kewaunee, these recovery
mechanisms were:

- independent sign-off check by a second operator - 0.1;
- presence of a compelling sigual indicating that the component is incorrectly positioned - 0.1; and
- performance of functional test following maintenance - 0.01.

The one exception to the documented ASEP HRA method was an additional recovery mechanism for the potential that a valve mispositioned after testing while at power may be detected and corrected during periodic operator walk-round checks. The effect of the walk-round checks is to reduce the mean time that the equipment would be unavailable because of the mispositioned valve. For example, if a valve was tested quarterly and left mispositioned and undetected, the equipment would be unavailable until the next quarterly test. However, with intermediate walk-round checks, the valve position would most likely be detected and corrected. Using this logic, the unavailability of such valves was reduced in the ratio of the time between walk-rounds to the time between tests, with a limit of 0.05 (i.e., no more than 20 walk-downs between tests). This calculation process was recommended to the licensee by Dr. Gareth Parry, NUS Corporation, who acted as a consultant to the revised HRA task.

Pre-initiator human actions are identified as contributors in two of the top 100 dominant cut-sets:

1. Failure to restore the TSC diesel generator after test (10-GE-TSC-DG-AE): This action is a contributor to the 19th dominant cut-set, with a core-damage frequency contribution of 7.3E-07 per year (0.69% of the total core-damage frequency); and

2. Miscalibration of the RWST level instruments (33RTL--RWST--AE): This action is a contributor to the 41st dominant cut-set, with a core-damage frequency contribution of 2.1E-07 per year (0.22% of the total core-damage frequency).

In addition to the listing of dominant cut-sets, the licensee has presented risk-increase and risk-decrease importance measures for basic events, including human actions. Of the events having the top 100 risk-increase importance measures, three are associated with pre-initiator human actions:

1. Miscalibration of the RWST level instruments (33RTL--RWST--AE): This action has the 30th highest risk-increase importance measure;

2. Failure to open AOV AFW-2B after test (05BAV--AFW2B-AE): This action has the 76th highest risk-increase importance measure;

3. Failure to open AOV AFW-2A after test (05BAV--AFW2A-AE): This action has the 98th highest risk-increase importance measure.

Of the events having the top 100 risk-decrease importance measures, four are associated with pre- initiator human actions. These are:

1. Failure to restore the TSC diesel generator after test (10-GE-TSC-DG-AE): This action has the 40th highest risk-decrease importance measure;

2. Failure to open manual valve CC-4B after test (31-XV---CC4B-AE): This action has the 74th highest risk-decrease importance measure;

3. Miscalibration of the RWST level instruments (33RTL--RWST--AE): This action has the 82th highest risk-decrease importance measure;

4. Failure to restore diesel generator A after test (10-GE-DG1A---AE): This action has the 97th highest risk-decrease importance measure.

In addition, the licensee performed a sensitivity analysis for the pre-initiator human actions, by systematically increasing and decreasing the probabilities of all such actions by a factor of 10. The effect of increasing the probabilities by a factor of 10 was to increase the core-damage frequency by a factor of 1.5 (from 1.05E-04/yr to 1.5E-04/yr). Decreasing the probabilities by a factor of 10 reduced the core-damage frequency by a factor of 0.96, from 1.05E-04/yr to 1.0E-04/yr.

3. Analysis of Post-Initiator Human Actions

The licensee has reanalyzed the post-initiator human actions using two methods: one for failures in detection, diagnosis and decision-making (also identified by the licensee as "cognitive" failures) and one for failures in task execution. The Cause-Based Decision Tree (CBDT) Method developed by the Electric Power Research Institute (EPRI)[1] was used to quantify the likelihood of errors in detection, diagnosis and decision-making. This method was developed as a supplementary method to other EPRI HRA methods for use when use of the time-based methods like the Human Cognitive Reliability (HCR) and Operator Reliability Experiment (ORE) methods were judged to provide inappropriate human error probabilities. In the revised analysis, the licensee modeled a total of 42 post-initiator response actions, 6 recovery actions, and 15 response actions to be taken in the event of internal fire events.

The CBDT method uses a set of decision trees to model errors in the cognitive element of each action and recommends use of the THERP method to model the failures to perform the task-execution portion of the action. The failure probability for the action is calculated as the sum of the cognitive and task-execution portions of the action.

This method estimates failure probabilities for the cognitive elements based on an assessment of the following eight factors:

1. availability of relevant indications (location, accuracy, reliability of indications);
2. attention to indications (workload, monitoring requirements, relevant alarms, etc.);
3. data errors (location on panel, quality of display, interpersonal communications);
4. misleading data (cues match procedure, training in cue recognition, etc.);
5. procedure format (visibility and salience of instructions, place-keeping aids);
6. instructional clarity (standardized vocabulary, completeness of information, training provided);
7. instructional complexity (use of "not" statements, complex use of "and" & "or" terms, etc.); and
8. potential for deliberate violations (belief in instructional adequacy, availability and consequences of alternatives, etc.).

Recovery factors, such as reviews by other crew members, including the shift technical advisor (STA), are allowed to reduce the error probabilities calculated from the decision trees if there is sufficient time. The criterion of "sufficient time" depends on the particular recovery factor--for example, credit for review by the STA is not permitted unless there is at least 15 minutes

---

. EPRI TR-100259, An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment, Electric Power Research Institute, Palo Alto, CA, June 1992.

from the initiating cues for the operator actions to be completed. In contrast to the other EPRI HRA methods, the CBDT method does not otherwise directly incorporate measures of time in quantifying human error probabilities.

The likelihoods of failures in task execution were quantified using the THERP method, described in NUREG/CR-1278[2]. The analysis of task-execution actions relied on a subset of the THERP method, focusing on five basic types of errors:

- errors of omission involving skipping steps in written procedures, based on Table 20-7 of NUREG/CR-1278;
- errors of commission in reading and recording quantitative information from unannunciated displays, based on Table 20-10 of NUREG/CR-1278;
- errors of commission in check-reading displays, based on Table 20-11 of NUREG/CR-1278;
- errors of commission in selecting and operating manual controls, based on Table 20-12 of NUREG/CR-1278; and
- errors in the selection and operation of locally operated valves, based on Table 20-13 of NUREG/CR-1278.

These types of errors represent most types of errors in task-execution covered by the THERP method, though errors of commission in selecting unannunciated displays for quantitative or qualitative readings (Table 20-9 of NUREG/CR-1278) are omitted. Provided the Kewaunee control- room interfaces are well designed, using clearly drawn mimic lines to indicate relationships of displays to systems, or the displays involved are of dissimilar appearance to other adjacent displays, the omission of this type of error is unlikely to be significant. In the original IPE submittal (item 10, page 328), the licensee indicated that the control-room interface design generally does use mimic lines, though individnal displays are not discussed. It is therefore considered unlikely that the omission of this type of error will result in failure to identify plant vulnerabilities or in distortions of contributors to the frequency of core damage.

Compared with the method used in the original Kewaunee IPE submittal, it is considered that, in principle, the combination of the CBDT method and THERP does provide a more realistic basis for assessing post-initiator human actions, including its consideration of plant-specific PSFs and the incorporation of dependencies.

However, the CBDT method does not, in itself, identify and analyze time-critical actions--that is, those actions where the difference between the time available and the time required to

---

NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, A.D. Swain & H.E. Guttmann, Sandia National Laboratories, Albuquerque, NM, August 1983.

perform the actions is short and the possibility exists for the operators to fail to accomplish the actions in time is significant. While the licensee has provided estimates of the time available to perform many of the actions, there is no indication of the time required to perform the actions, and therefore it is not possible to identify which actions are in fact time-critical. The CBDT method implicitly incorporates the effects of time availability through the application of recovery factors only if there is "time available". For example, if more than 15 minutes is available, the possibility of error detection and correction by the shift technical advisor may be credited as a recovery factor.

The licensee implies that the only direct effect of time availability is when the time available to perform an action is less than the time required to perform the action, in which case a failure probability of 1.0 is assigned. [The licensee actually states the reverse of this relationship--no credit if the time available is greater than the time required (item 4, page 4.15.1-7 of the revised HRA submittal).]

In a limited number of cases, the cognitive portion of the human action was not modeled--for example, the post-ATWS actions to trip the reactor manually (MRT), to de-energize buses 33 and 43 that supply the control-rod drive motor/generator sets (ORT), or to achieve long-term shut-down (LTS). In the case of an ATWS, the licensee states that "it is obvious that an ATWS has occurred, so diagnosis is ignored ...".

The licensee made several assumptions in applying the THERP method to the task-execution portion of the human actions. These include:

- an error probability calculated to be less than 1.0E-04 is rounded up to the value of 1.0E-04;
- the probability of skipping a step in a procedure presented in Table 20-7 of NUREG/CR-1278 can be reduced by a factor of 3 when the procedural format is in a columnar format rather than a narrative format (this adjustment is supported by the method's authors on page 15-15 of NUREG/CR-1278);
- recovery by an operator from an omitted procedural step can be allowed if the procedure later directs the operator to check the function addressed in the earlier step, and the check step is not on the same page as the initial step;
- at least a moderately high level of stress is assumed for all post-initiator actions, and that extremely high stress is assumed in most cases where the operators are applying the functional restoration (FR) or emergency condition action (ECA) procedures.

Dependencies in post-initiator human actions are described as being considered explicitly, based generally of the following four assumptions:

1. all task-execution actions are completely dependent on successful diagnosis;

2. two failures separated in time by a successful action are independent;
3. dependence between an error and a subsequent check step or recovery step in a procedure is dependent on the number of steps and is assessed on a case-by-case basis, with actions on the same page being considered completely dependent; and
4. memorized immediate action steps of EOP E-0 or ECA-0.0 are independent of actions taken later in the procedure.

Using these assumptions, five sets of actions were modeled as having dependent relationships:

- depressurize RCS to stop tube leak and cool down & depressurize RCS in EOP ECA-3.1 (low dependency);
- isolate AOV MU-3A during station blackout and establish charging flow during blackout (dependency based on page in procedure);
- open battery room doors for ventilation and open doors for AFW ventilation (moderate dependency);
- isolate RHR pumps and throttle SI flow (moderate dependency); and
- isolate break and throttle SI flow (moderate dependency).

However it is noted that other actions that might be considered potentially dependent are not discussed. For example, the actions MRT, ORT, and LTS identified earlier, to ensure that the reactor is shutdown in the event of an ATWS, are considered independent. The joint probability of these three actions is 1.3E-08. There is no discussion as to why these actions should be considered to be independent, given their being required in a short time-frame and are in response to the same accident condition.

The licensee analyzed six actions to recover equipment that failed to start or change state automatically when required in an accident sequence, including two actions associated with protecting the containment integrity as part of the level 2 component of the IPE. Most of the recovery actions consist of separate steps when following emergency operating procedure (EOP) E-0, and are modeled as task-execution failures in performing the appropriate action. Diagnosis failures are considered only for the action to start containment spray (231-MAN-ICS--HE) in response to the EOP FR-Z.1, Response to High Containment Pressure.

In addition, the licensee modeled 15 human actions that could occur during internal fires, modeled as part of the IPE related to external events. For the most part, similar actions are modeled for fires that occur in two redundant locations: the "dedicated zone" and the "alternate zone". The actions are to establish the functions associated with the following systems: service water, diesel generator, containment fan cooling, auxiliary feedwater, component cooling water, containment isolation, and safety injection/charging. In addition, actions to establish instrument air are included for the fires in the dedicated zone. The actions in the event of fire are modeled using the same general methods as the other post-initiator human actions.

Post-initiator human actions provide a significant contribution to the core-damage frequency of Kewaunee. Of the top 100 dominant cut-sets, 44 involve one or more post-initiator human actions, and these cutsets make up approximately 56% of the total core-damage frequency. The human actions that are part of the cut-sets contributing at least 1% of the core damage frequency are:

1. Operator fails to stop both RHR pumps in EOP E-1, small & medium LOCAs (34I- RHR-STE1-HE). This action contributes to the top two cut-sets that, together, comprise approximately 27% of the total core-damage frequency for Kewaunee;

2. Operator fails to cool down and depressurize RCS to stop tube leak, steam generator tube rupture (06--OS1------HE). This action (together with the next item in this list) contributes to the third dominant cut-set, comprising 8% of the core-damage frequency;

3. Operator fails to cool down and depressurize RCS in ECA-3.1/3.2, steam generator tube rupture (35--EC3-----DHE). This action (together with the previous item in this list) contributes to the third dominant cut-set, comprising 8% of the core-damage frequency;

4. Operator fails to establish recirculation (1 of 2 trains), medium LOCA (33R-2TRN- REC-HE). This action contributes to the fifth dominant cut-set, comprising approximately 5% of the core damage frequency;

5. Operator fails to establish charging flow during blackout, station blackout (35--CHB------HE). This action contributes to the eighth dominant cut-set, comprising approximately 2.6% of the core-damage frequency;

6. Operator fails to stop both RHR pumps in EOP FR-H.1, transient without feedwater (34I-RHR-STH1-HE). This action contributes to the ninth dominant cut-set, comprising approximately 2.5% of the core-damage frequency;

7. Operator fails to diagnose steam generator tube rupture, steam generator tube rupture (36--SGR-DIAG-HE). This action contributes to the 12th dominant cut-set, comprising approximately 1.4% of the core-damage frequency;

8. Operator fails to establish low pressure recirculation, large LOCA (34R-LR1------HE). This action contributes to the 14th dominant cut-set, comprising approximately 1.1% of the core-damage frequency; and

9. Operator fails to stop reactor coolant pumps, transient with main feedwater (36-RXCP-STOP-HE). This action contributes to the 16th dominant cut-set, comprising approximately 1 % of the core-damage frequency.

The licensee performed assessments of the risk-increase and risk-decrease importances of the post- initiator human actions. Six actions were found to have risk-increase importances ranked in the top hundred events. These are:

1. Operator fails to stop both RHR pumps in EOP E-1. This action has the 18th highest risk-increase importance measure;

2. Operator fails to diagnose steam generator tube rupture. This action has the 23rd highest risk-increase importance measure;

3. Operator fails to establish recirculation (1 of 2 trains). This action has the 32nd highest risk-increase importance measure;

4. Operator fails to stop reactor coolant pumps. This action has the 38th highest risk- increase importance measure;

5. Operator fails to cool down and depressurize RCS to stop tube leak. This action has the 53rd highest risk-increase importance measure; and

6. Operator fails to establish low pressure recirculation. This action has the 62nd highest risk-increase importance measure.

Eighteen actions were found to have risk-decrease importances ranked in the top hundred events. The most important of these are:

1. Operator fails to stop both RHR pumps in EOP E-1. This action has the 2nd highest risk-decrease importance measure.

2. Operator fails to cool down and depressurize RCS to stop tube leak. This action has the 7th highest risk-increase importance measure.

3. Operator fails to cool down and depressurize RCS in ECA-3.1/3.2. This action has the 9th highest risk-increase importance measure.

4. Operator fails to stop both RHR pumps in EOP FR-H.1. This action has the 10th highest risk-increase importance measure.

5. Operator fails to establish recirculation (1 of 2 trains). This action has the 14th highest risk-increase importance measure.

6. Operator fails to establish charging flow during blackout. This action has the 20th highest risk-increase importance measure.

The licensee performed a sensitivity analysis for the post-initiator human actions, by systematically increasing and decreasing the probabilities of all such actions by a factor of 10. The effect of increasing the probabilities by a factor of 10 was to increase the core-damage frequency by a factor of 7.6 (from 1.05E-04/yr to 8.0E-04/yr). Decreasing the probabilities by a factor of 10 reduced the core-damage frequency by a factor of 0.44, from 1.05E-04/yr to 4.6E-05/yr.

4. Summary of Results of Requantification

The overall effect of the requantification is to increase the contribution to the frequency of the Kewaunee core damage from human actions. The results provided by the licensee indicate that using the revised HRA values increased the total CDF approximately 58% over the frequency of identified in the original submittal, to a new total core damage frequency of 1.05E-04/yr.

In the initial submittal, the licensee identified that post-initiator human actions provided a significant contribution to the Kewaunee core-damage frequency; of the top 13 core-damage sequences that contributed 85% of the original core-damage frequency, four involved failures in human actions, some with more than one failure. These human actions were:

1. Operators fail to cool down and depressurize the RCS following a small LOCA;

2. Operators fail to accomplish high- or low-pressure sump recirculation following a small LOCA;

3. Operators fail to cool down and depressurize the RCS initially following a steam generator tube rupture;

4. Operators fail to cool down and depressurize the RCS to atmospheric pressure following a steam generator tube rupture;

5. Operators fail to accomplish feed-and-bleed cooling following a loss-of-offsite-power event;

6. Operators fail to accomplish recirculation cooling following a large LOCA.

Several of the human actions in these dominant sequences are similar to the human actions associated with dominant cut-sets in the reanalysis. However, the largest contribution in the reanalysis from human actions (failure to stop both RHR pumps in small and medium LOCAs, 27% of the core-damage frequency) was not identified as significant in the original analysis.

The licensee has not provided any discussion of the influence of the reanalysis on the identification of vulnerabilities presented in Section 3.4.3 of the original submittal.

5. Observations

The licensee has made the following changes to the Kewaunee HRA:

i. explicit incorporation of failures in the decisionmaking as well as the task-execution portion of the human actions;

ii. explicit inclusion of plant-specific and event specific shaping factors in the assessment of post-initiator human actions;

iii. elimination of the use of the "special, one-of-a-kind" checking as a recovery factor and the arbitrary reduction of a factor of 10 for errors of commission in the execution portion of the human action; and

iv. analysis of a limited number of pre-initiator calibration actions.

The methods used to quantify the two portions of the human actions (decisionmaking and task execution) are considered appropriate for their purposes in this analysis. In particular, the CBDT method incorporates several performance-shaping factors related to decisionmaking activities, and were developed from psychological models as described in Reference 1. The use of this method to quantify the decisionmaking element of the post-initiator actions therefore removes one of the major limitations of the HRA portion of the Kewaunee submittal.

In itself, use of the CBDT method does not resolve directly all of the concerns associated with the modeling of post-initiator actions. In particular, time as a shaping factor is modeled only indirectly, in terms as of the existence of recovery factors (such as checking by other crew members or self- checking).

In the revised Kewaunee submittal, the licensee does present some information concerning the time available for performing actions, but no information is provided concerning the time required physically to accomplish the actions, so it is not possible to identify whether any actions have only a very short window to start taking the necessary steps. Such situations might lead to underestimates of the failure probability because the CBDT method and THERP do not model

explicitly failures from the actions not being completed in time.

The licensee did add a set of human reliability analyses for five miscalibration events. These include miscalibration of the RWST tank level that has been shown as potentially significant in other IPEs. However, no basis is presented by the licensee as to why the five miscalibration events represent the only events needing analysis.

One final observation is that there are several typographical errors and mis-statements in the revised submittal. In themselves these are not considered significant. However, they indicate a possible weakness in proofing and internal review of the document, which raises the possibility that technical errors exist in the results of the HRA or the identification of important sequences, and would not be identified by this review. Examples of errors found in the review are:

- "If time available for the HI [human interaction] is greater than the estimated time to perform it, the HI is considered to fail and no credit is taken for it." (Item 4, page 4.15.1-7). This is the inverse of the actual analysis and is logically absurd.
- Items 1. and 9. in the list of guidelines for assessing dependencies are identical ("Two failures separated in time by an essential successful action are regarded as independent." pages 4.14.1-8 and -9).
- Dr Gareth Parry, consultant for the HRA reanalysis, is repeatedly mis-identified as Mr. Gareth Perry.