CONCORD ASSOCIATES, INC.

Systems Performance Engineers

FORT CALHOUN STATION

TECHNICAL EVALUATION REPORT ON THE IPE SUBMITTAL HUMAN RELIABILITY ANALYSIS

FINAL REPORT

by

John Wreathall
John Wreathall & Company, Inc.

Prepared for

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

Final Report, September 5, 1996

11915 Cheviot Dr.	725 Pellissippi Parkway	6201 Picketts Lake Dr.
Herndon, VA 22070	Knoxville, TN 37932	Acworth, GA 30101
(703) 318-9262	(615) 675-0930	(404) 917-0690

FORT CALHOUN STATION

TECHNICAL EVALUATION REPORT ON THE IPE SUBMITTAL HUMAN RELIABILITY ANALYSIS

.

FINAL REPORT

John Wreathall
John Wreathall & Company, Inc.

Prepared for

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

Final Report, September 5, 1996

TABLE OF CONTENTS

Table of Contents (continued)

TABLES

FIGURES

E.   EXECUTIVE SUMMARY

This Technical Evaluation Report (TER) is a summary of the documentation-only review of the human reliability analysis (HRA) presented as part of the Omaha Public Power District's Individual Plant Examination (IPE) submittal for the Fort Calhoun Station (FCS) to the U.S. Nuclear Regulatory Commission (NRC). 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.

E.1   Plant Characterization

Ft. Calhoun Station (FCS) is comprised of a single-unit station, rated at 501 Mwe, and is located on the Missouri River approximately 19 miles north of Omaha, Nebraska. It is owned and operated by the Omaha Public Power District (OPPD). The reactor is a Combustion-Engineering-supplied pressurized water reactor (PWR). The plant began commercial operation in September 1973.

The licensee notes several plant characteristics that described as important factors related to the reliability of plant personnel. These are:

1)   The inventory of the steam generators at FCS are relatively large, which allows an extended period of time for the operators to accomplish feed-and-bleed operations if required.

2)   The transfer of safety-injection and containment-spray systems from injection to recirculation is accomplished entirely from the control room; no ex-control-room actions are required.

3)   FCS is characterized as a "relatively compact" plant. Areas outside the control room in which ex-control-room actions would be performed can be reached quickly and easily, which increases the probability that an action would be successfully performed within the allowable time period.

E.2   Licensee IPE Process

The FCS IPE is comprised of a Level 1, Level 2, and a Level 3 PRA with internal flooding analysis. The HRA process addressed both ¡ e-initiator and post-initiator human actions. The analysis of pre-initiator actions included both restoration errors and miscalibration errors; the licensee refers to pre-initiator actions as "maintenance, test and calibration (MTC) errors." The analysis of post-initiator human actions included response- and recovery-type actions; the licensee refers to all post-initiator actions as "recovery actions" regardless of whether they are proceduralized or not. Post-initiator human actions were included in the analysis of internal floods. One human action was identified in the analysis of containment performance, to recover containment spray following vessel failure.

The modeling of human actions in the FCS IPE distinguished between two kinds of human errors: slips and mistakes. The distinction between these two kinds of errors is one of intention. A slip occurs when the outcome of the action is not what the operator intended; for example, selecting the wrong switch or inadvertently skipping a step in a procedure are typical slips. In contrast, a mistake involves actions taken that the operator intended, but the intention is flawed. Isolating the wrong steam generator in the mistaken belief that it (and not the failed steam generator) has ruptured is an example of a mistake. The analysis of pre-initiator human actions in the FCS IPE is confined to slips. The analysis of the post-initiator human actions includes both slips and mistakes. Slips are modeled using a simplified version of THERP and mistakes are modeled using a set of time/reliability correlations.

The HRA task was performed as part of the Level 1 PRA. The submittal identifies that the Level 1 PRA was largely performed by the licensee's PRA Group, which included plant personnel with 65 years of accumulated FCS plant experience and included the presence of a senior reactor operator (SRO). This work of this group involved extensive interfacing and review with personnel from the Licensee's Production Engineering Division, and operations, maintenance training, and reliability engineering personnel. Three levels of review were provided for the IPE, including the HRA tasks. The first level was provided by a PRA Oversight Committee, staffed by licensee personnel from several departments including licensing, training and operations; this committee helped to ensure the technical accuracy of the models. The second level of review, provided by the PRA Executive Committee comprised of senior licensee management, was responsible for reviewing any significant PRA findings and their resolution. The third level of review was provided by people external to the licensee, and was comprised of staff from Duke Engineering, Yankee Atomic Electric Company, and ABB/Combustion Engineering. As part of the Level 1 PRA, the licensee performed both importance and sensitivity analyses. These were used by the licensee as the primary basis to identify which human actions were considered important to the frequency of core damage at FCS.

E.3   Human Reliability Analysis

E.3.1   Pre-Initiator Human Actions.

The licensee included consideration of: (1) failures of plant personnel to restore components and systems following testing and maintenance, and (2) failures during calibration of instrumentation and control equipment. These failures represent an appropriate range of pre-initiator human actions.

No explicit description of the process for the initial identification of pre-initiator human actions was provided in the licensee's information. However the following is inferred from the description of the systems analysis and the description of information used in the IPE.

First, systems that could influence the development of accident sequences were identified and selected as part of the front-end analysis. For each such system, detailed systems'

analysis notebooks were prepared. These included identification of all components whose states were changed during testing and maintenance, as defined in the FCS test and maintenance procedures. Those components whose changes of state during testing and maintenance could lead to system or train failures (within the definition of the system fault trees) were then reviewed using a quantitative screening process to identify those pre-initiator human actions to be subject to detailed HRA quantification modeling.

The screening analysis for pre-initiator human actions mostly comprised assigning a failure probability of 3.0E-03 for actions associated with single components and 3.0E-04 for actions associated with multiple redundant components. Components subjected to functional testing following test or maintenance had lower screening probabilities assigned. Following the screening analysis, 17 pre-initiator human actions were identified for detailed modeling.

Detailed modeling of the pre-initiator human actions was performed using a simplified model based on the Technique for Human Error Rate Prediction (THERP). The model was simplified by taking into account only the following factors: (1) number and redundancy of components affected, and (2) interpersonal dependencies. The model allows for adjustments for other performance-shaping factors, but these do not appear to have been used in the actual application.

Of the 17 human actions modeled in detail, two were identified through the sensitivity analysis as having the potential for contributing significantly to the core-damage frequency. These are:

1) GHFLPRESS – Human miscalibrates Safety Injection Refueling Water Tank (SIRWT) level pressure switches and transfer to recirculation occurs too soon; and

2) KJUMPER – Failure to remove RPS interposing relay jumpers prior to power operations.

E.3.2 Post-Initiator Human Actions.

The analysis of post-initiator human actions included response- and recovery-type actions; the licensee refers to all post-initiator actions as "recovery actions" regardless of whether they are proceduralized or not. The analysis of post-initiator human actions included the modeling of both slips and mistakes as described above. A limited number of actions are associated with internal floods and one action is associated with preserving the integrity of the containment in the post-core-damage phase of the accident.

As with the pre-initiator human actions, the licensee provides no explicit descriptions of the process used to identify post-initiator human actions for analysis. However, data sources used to identify these actions included the emergency and abnormal operating procedures (EOPs and AOPs), walk-downs of the plant and control facilities, and discussions with plant and training personnel. It is noted that the licensee's HRA team did include a senior reactor operator.

Separate screening processes were used for slips and mistakes in the analysis of post-initiator human actions. In the case of slips, a single failure probability of 1.0 was assigned as the screening value, and a single failure probability of 0.4 was assigned for mistakes. As a result, 19 post-initiator slips and 25 mistakes were identified for detailed modeling.

The detailed modeling of slips was performed using the same model as was used for the pre-initiator human actions.

Of the 19 post-initiator slips, five were identified in sensitivity analysis as having the potential for providing a significant contribution to the core-damage frequency. These are:

1) OPER-41 – failure to make up to the emergency feedwater storage tank (EFWST) with the diesel-driven auxiliary feedwater pump;

2) OPER-70 – failure to depressurize the reactor coolant system (RCS) in response to an interfacing systems loss-off-coolant accident (ISLOCA);

3) EHFFEOP-00 – failure to reload equipment (such as air compressors) following loss-of-offsite power, as required in post-trip procedure EOP-00;

4) OPER-9 – failure to depressurize and terminate RCS primary-secondary leakage following a steam-generator tube rupture (SGTR); and

5) AHFFCONTROL – failure to control auxiliary feedwater (AFW) flow and prevent flooding of the steam-driven AFW pump.

In addition, the importance-measure analysis identified one post-initiator slip as having the third-highest Fussel-Vesely importance measure; this is event OPER-41 described above.

The detailed modeling of mistakes was performed using a set of time/reliability correlations. The set of time/reliability correlations cover four different types of actions:

1) verification actions: actions that simply involve verification within the control room;

2) rule-based actions: actions taken within the control room in accordance with the symptom-based emergency operating procedures (EOPs), are actions extensively rehearsed in training, and are associated with events for which the symptoms are very clear;

3) other response actions: actions taken within the control room generally in accordance with procedures or the knowledge of the operators; and

4) ex-control-room actions: response actions involving operator actions taken outside of the control room.

Two parameters dominate the quantification process: (1) the time available for operators to perform the necessary actions, and (2) the presence or absence of "burden". Burden is a concept that describes several reasons why operators may have difficulty or delay in

performing the necessary actions. Examples include a reluctance to perform particular tasks (such as feed-and-bleed), when symptoms are confusing, when access to a hostile environment is required, or when multiple faults are experienced.

Two post-initiator mistakes were identified in the sensitivity analysis as having the potential to significantly affect the core-damage frequency. These are:

- AHFFEFWST – failure to align makeup flow to the EFWST from any source (ex-control room); and
- OPER-4 – failure to initiate feed-and-bleed when required (rule-based, in control room).

In addition, two post-initiator mistakes were identified by the importance analysis as having the sixth- and eighth-highest Fussel-Vesely importance measures. These were respectively:

- XEFWST – failure to use diesel-driven fire pump to replenish the EFWST (ex-control room); and
- XBRKRTRIP – failure to manually trip 4160 VAC breaker given the breaker failed to trip automatically (rule-based, in control room).

E.4 Generic Issues and CPI

The licensee recognizes that human actions play an important role in preventing core damage from failures in the decay-heat-removal process. Two sets of actions are identified: (1) those to ensure that long-term heat removal via the steam generators can be maintained by refilling the EFWST, and (2) feed-and-bleed cooling if secondary-side cooling is lost. The licensee identified several means for the operators to replenish the inventory of the EFWST, including use of the fire-pump hook-up. The failure to line up flow to the EFWST within 8 hours involves actions outside of the control room, and is estimated to have a failure probability of 3.0E-03.

A total of nine human actions were associated with the modeling of internal flooding. Eight of the nine actions were events already identified in the internal-events analysis, and one new event unique to the internal-flooding analysis was identified. The quantification of the flood-related human actions was based on the internal-events HRA models, but included adjustments related to the accessibility of plant areas under flooding conditions.

Most of the dominant internal-flood sequences include combinations of human actions but no details of the relative contributions of these actions to the frequency of core damage from internal floods are provided.

In addition, one plant improvement was identified associated with internal floods. This is a modification of the procedure for responding to alarms associated with flooding in the safety-injection (SI) and containment-spray (CS) pump rooms. The submittal shows the

modification to be in progress.

No human actions were identified in relation to containment performance improvements.

E.5 Vulnerabilities and Plant Improvements

The licensee applied the criteria from NUMARC 91-04 as the basis for screening plant-specific vulnerabilities. Based on these criteria, three functional accident sequences were identified as having core-damage frequencies within the range 1E-5 to 1E-6 per year. These are:

1) TX – transient initiating event with failure of long-term heat removal;
2) TQ2U – transient-induced RCP seal LOCA with failure of high-pressure safety injection; and
3) TBF – transient initiating event followed by failures of primary-secondary heat removal and feed-and-bleed cooling.

Functional sequences TX and TBF involve human actions: initiating long-term heat removal and replenishing the EFWST in sequence TX, and establishing feed-and-bleed cooling in sequence TBF.

The licensee states that severe accident management guidelines (SAMGs) will be developed for these functional sequences to prevent or mitigate core damage, vessel failure, or containment failure, in accordance with the NUMARC guidance.

Two operator-related enhancements were identified as a result of performing the IPE. These were:

1) the addition of a manually closed door to permit access to isolate the component-cooling water system in the event of flooding from failure of a reactor coolant pump (RCP) seal cooler; and
2) modification of the procedure for responding to alarms associated with flooding in the safety-injection (SI) and containment-spray (CS) pump rooms, directing operators to open a water-tight door to allow drainage of the water from the equipment rooms, or to close the door for floods initiating in Room 23. (The door is normally open.)

The FCS submittal shows modification 1 as being complete and modification 2 in progress. The effect of modification 1 was credited in the IPE models. The internal-flooding analysis was performed assuming that the door in modification 2 was open.

E.6 Observations

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

Particular strengths in the FCS HRA analysis are considered to be:

1) The analysis includes explicit guidelines for the selection of models to be used in the quantification of human actions through the use of a decision tree.

2) The analysis describes how the human actions should be incorporated into the PRA logic models explicitly, and the final PRA models were reviewed by the HRA analyst to ensure that the human actions were incorporated appropriately.

3) The analysis does include all appropriate classes of human actions that are likely to contribute to the frequency of core damage (maintenance, test and calibration actions in the pre-accident phase, and failures in decision-making [mistakes] and task execution [slips] in the post-accident phase).

4) Explicit modeling of actions required to mitigate internal flooding was performed, including the incorporation of the effects of flooding on the operator actions.

5) One human action was identified as part of the containment-performance analysis. This action is to start manually containment sprays following their failure to initiate automatically following vessel breach, given that the containment-spray system is available at the onset of core damage.

6) This IPE is believed unique in that a limited number of potentially significant errors of commission were identified that have the potential to create new accident scenarios. While not quantifying these actions (because of a lack of any meaningful models with the current state-of-the-art in HRA), the analysis has at least recognized the possibility of such actions.

However, there appear to be certain limitations in the analysis. These include:

1) There is no case-by-case (plant-specific and event-specific) assessment of some of the factors influencing human actions to assure a completely realistic understanding of human performance in the plant. The analysis of pre- and post-initiator human actions does not include any consideration of the human-system interface or the procedures for example.

2) The quantification model used for slips contains limitations that may result in the under-estimation of the failure probabilities of both pre- and post-initiator human actions. In particular, the use of relatively low screening probabilities for pre-initiator slips could potentially lead to the omission of important actions from the detailed analyses. Additionally, the use of the simple model for the detailed analysis of slips could lead to the under-estimation of probabilities of failure for components that have plant-specific weaknesses associated with the human-system interface.

3) There are some characteristics associated with the modeling of mistakes that can lead to seemingly inconsistent results. The model uses different time/reliability correlations depending on whether actions are verification, rule-based, or "other" actions, whether they occur inside or outside the

control room, and whether the operators are burdened. Differences in the quantification results based on different assumptions can be significant. For example, there appears to be no specific guidance as to which actions should be assigned to include the burden factor; this factor can significantly affect the estimated failure probability. It is not possible to confirm the reasons for what can at times seem arbitrary assignments of the burden factor.

4) Some guidance is provided as to which actions should be modeled as slips or mistakes, but skilled judgments by the analyst are required. This demand could lead to limitations in future revisions of the FCS IPE if the analysts performing those revisions are not familiar with the judgments required in the analysis. However, the guidelines provided by the licensee appear reasonable in themselves.

5) The ex-control room time/reliability correlation leads to an estimated failure to accomplish long-term heat removal within 8 hours, of 2.1E-02. This probability, when compared with the reliability of other actions is considered disproportionately high. It is possible that this failure is one main reason why sequences initiated by transients and involving failure to accomplish long-term heat removal comprise such a large contribution (39%) to the frequency of core damage at FCS.

1. INTRODUCTION

1.1 Review Process

The HRA review was a "docume.it-only" process, which consisted of essentially four steps:

1) Comprehensive review of the IPE submittal focusing on al! information pertinent to HRA.

2) Preparation of a draft TER summarizing preliminary findings and conclusions, noting specific issues for which additional information was required from the licensee, and formulating requests to the licensee for the necessary additional information.

3) Review of preliminary findings, conclusions and proposed requests for add::ional information (RAIs) with NRC staff and with "front-end" and "back-end" reviewers.

4) Review of licensee responses to the NRC requests for additional information, and preparation of this final TER modifying the draft to incorporate results of the additional information provided by the licensee.

In addition, the licensee provided supplementary information that clarified the HRA methodology used in the IPE.

Findings and conclusions are limited to those that could be supported by the document-only review. No visit to the site was conducted. In general it was not possible, and it was not the intent of the review, to reproduce results or verify in detail the licensee's HRA quantification process.

1.2 Plant Characterization

Ft. Calhoun Station (FCS) is comprised of a single-unit station, rated at 501 Mwe, and is located on the Missouri River approximately 19 miles north of Omaha, Nebraska. It is owned and operated by the Omaha Public Power District (OPPD). The reactor is a Combustion-Engineering-supplied pressurized water reactor (PWR). The plant began commercial operation in September 1973.

The licensee notes several plant characteristics that described as important factors related to the reliability of plant personnel. These are summarized as follows:

1) The inventory of the steam generators at FCS are relatively large, which allows an extended period of time to accomplish feed-and-bleed operations if required.

2) The transfer of safety-injection and containment-spray systems from injection to recirculation is accomplished entirely from the control room; no ex-control-room actions are required.

3)   FCS is characterized as a "relatively compact" plant. Areas outside the
      control room in which ex-control-room actions would be performed can be
      reached quickly and easily, which increases the probability that an action
      would be successfully performed within the allowable time period.

Very limited information is provided in the FCS IPE Submittal and the response to the
RAI concerning the human-performance-related characteristics of the plant. Other than
identifying Abnormal, Emergency, and Maintenance Procedures, and Operating
Instructions as source of information for the study, there is no description of the plant-
specific human-performance-related factors being assessed or used in the HRA
quantification.

2.   TECHNICAL REVIEW

2.1   Licensee IPE Process

The FCS IPE is comprised of a Level 1, Level 2, and a Level 3 PRA with internal flooding analysis. The HRA process addressed both pre-initiator and post-initiator human actions. The analysis of pre-initiator actions included both restoration errors and miscalibration errors; the licensee refers to pre-initiator actions as "maintenance, test and calibration (MTC) errors." The analysis of post-initiator human actions included response- and recovery-type actions; the licensee refers to all post-initiator actions as "recovery actions" regardless of whether they are proceduralized or not. Post-initiator human actions were included in the analysis of internal floods. One human action was identified in the analysis of containment performance, to recover containment spray following vessel failure.

The modeling of human actions in the FCS IPE distinguished between two kinds of human errors: slips and mistakes. The distinction between these two kinds of errors was observed by Reason and Mycielska [1] as related to one of intention. A slip occurs when the outcome of the action is not what the operator intended; for example, selecting the wrong switch or inadvertently skipping a step in a procedure are typical slips. In contrast, a mistake involves actions taken that the operator intended, but the intention is flawed. Isolating the wrong steam generator in the mistaken belief that it (and not the failed steam generator) has ruptured is an example of a mistake. The analysis of pre-initiator human actions in the FCS IPE is confined to slips. The analysis of the post-initiator human actions includes both slips and mistakes. Slips are modeled using a simplified version of THERP and mistakes are modeled using a set of time/reliability correlations.

The HRA task was performed as part of the Level 1 PRA. The submittal identifies that the Level 1 PRA involved extensive interfacing and review with personnel from the Licensee's Production Engineering Division, and operations, maintenance and reliability engineering personnel. No role of plant personnel in the HRA task is described explicitly. The licensee's team was augmented by contractors and consultants; in particular SAIC performed the initial Level 1 PRA work, including the HRA modeling.

Three levels of review were provided for the IPE. The first level was provided by a PRA Oversight Committee staffed by licensee personnel from several departments including licensing, training and operations; this committee helped to ensure the technical accuracy of the models. The second level of review, provided by the PRA Executive Committee comprised of senior licensee management, was associated with reviewing any significant PRA findings and their resolution. The third level of review was provided by people external to the licensee, and was comprised of staff from Duke Engineering, Yankee Atomic, and ABB/Combustion Engineering. The HRA analyses are identified as being reviewed by all three levels.

2.1.1   Completeness and Methodology.

The FCS human reliability analysis covered all types of human actions normally included in PRAs. Specifically, the analysis included slips occurring in the pre-initiator phase, and slips and mistakes occurring in the post-accident phase. Some human actions were modeled that were associated with the internal flooding, and there was one human action associated with the Level 2 analysis.

Different models were applied for the analysis of slips and mistakes. Both models have been developed and applied in some other PRAs performed by SAIC; the submittal identifies these two models as parts of the SAIC HRA method. This method has been generally documented in a book by Dougherty and Fragola: *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications* [2]. Subsequently, some modifications have been made and incorporated in the method as applied in the FCS IPE.

The SAIC HRA method as described in the submittal comprises four elements: two quantification models for slips and mistakes, a decision tree for selecting which model to apply to a particular human action, and guidelines for incorporating the HRA results into the PRA logic models.

2.1.1.1 The Analysis of Slips. The analysis of slips is performed using a simplified version of the THERP HRA method.

Screening Analysis. In this model, screening values are assigned to slips according to when they occur, the number of components involved and the type of testing that may detect the failures. For the pre-initiator human actions, a basic failure corresponding to failure of a single component without full functional testing is used, with adjustment factors for multiple components and for full functional testing. A single value of 1.0 is used for screening post-initiator slips. Table 2-1 presents the values used in the method as implemented in the FCS IPE.

Table 2-1. Screening probabilities for slips.

Type of Human Action	Failure Probability
Pre-Initiator Actions	
Basic failure associated with single component	0.003
Factor when failure affects single component, following full functional test of component	0.1
Factor when failure affects multiple components	0.1
Factor when failure affects multiple components, following full functional test of components	0.02
Post-Initiator Actions	
Slips	1.0

4

Detailed Analysis. In the detailed modeling of pre-initiator slips, a single basic failure probability is assigned initially, and then factors are used to account for the number of trains affected, the number of people who may potentially correct the failure, and any other performance-shaping factors (PSFs). The general form of this equation is:

$$HFP = P_{nom} \times \beta \times \text{dependency factors} \times \Pi \text{ (PSFs)} \tag{2.1}$$

where:

HFP =	calculated human failure probability
P_{nom} =	nominal failure probability (0.003)
β =	beta factor, applied for multiple trains (0.1)
dependency factors =	adjustments for interpersonal dependency
PSFs =	other performance-shaping factors.

The dependency factors are approximations of the values presented by Swain and Guttmann in Table 20-21 of [3], and are assigned according the analyst's judgment of the level of dependency between the staff. Table 2-2 presents the default values used for the dependency factors in the FCS IPE.

Table 2-2. Default values for dependency factors.

Personnel	Dependency Level	Dependency Factor
Second licensed operator	complete	1.0
Licensed senior operator	high	0.5
Shift technical operator	moderate (in relation to cues)	0.14
Shift supervisor	moderate (after 1 hour)	0.14
Technical support center	high (after 1 hour)	0.5

While "other performance-shaping factors" are identified in Equation 2.1, none are identified as being used, with one exception. In the FCS IPE, a factor of 0.1 is applied to the estimation of the likelihood of miscalibration of the safety injection refueling water tank (SIRWT) level indicators, "to account for the fact that only gross miscalibration could fail the indicator's mission and the nominal HFP seems to better apply to slight miscalibrations." In other words, the model as used in the FCS IPE takes no account of any plant-specific human-factors characteristics; this is considered a limitation in the IPE.

2.1.1.2 The Analysis of Mistakes. The analysis of mistakes in the FCS IPE was performed using a set of time/reliability correlations. Time/reliability correlations represent one general means used in HRA methods for quantifying the failure probability of post-initiator human actions using parameters associated with the time that operators

5

have available to accomplish the necessary actions to prevent significant plant damage such as core-fuel damage. Different HRA methods use different combinations of parameters. The time used in the SAIC correlations is the time available for operators to perform actions before the onset of significant plant damage.

The set of time/reliability correlations described in [2] are associated with two sets of conditions: whether the actions are response actions (actions taken on the basis of procedures) or recovery actions (actions taken on an ad-hoc basis), and whether the actions are judged to involve hesitancy or not on the part of the operators. Hesitancy represents the potential for a delay in the response by operators because of ambiguity in the indications or the reluctance to take an action because of its potential consequences. Hence four time/reliability correlations are used representing the combinations of response or recovery actions, each with or without hesitancy.

Subsequent to the publication of [2], the method has been modified and expanded to add time/reliability correlations associated with actions taken outside the control room, and to include actions that simply involve verification (i.e., actions that confirm the operation of equipment). However the response action to scram manually the reactor in the event of an ATWS event has been modeled using the verification time/reliability correlation in the FCS IPE. As a result, the action is modeled with an effective failure probability of 0.0 (event XMANTRIP).

In addition, the time/reliability correlations used to model response actions have been divided to represent what the method describes as "rule-based" actions and "other" response actions. The time/reliability correlations associated with rule-based actions are used for those actions taken in accordance with the symptom-based emergency operating procedures (EOPs), are actions extensively rehearsed in training, and are associated with events for which the symptoms are very clear. In the FCS IPE, some post-initiator human actions were modeled using the rule-based time/reliability correlations and some using the "other response" time/reliability correlations. An example of a rule-based action in the FCS IPE is the initiation of feed-and-bleed cooling, and an example of an "other response" action is to trip a particular 4kV circuit breaker.

Recovery actions used in the initial model appear to have been dropped from the method as applied in the FCS IPE, though it is possible that the recovery-action time/reliability correlations have been incorporated into the ex-control-room time/reliability correlations, since most recovery actions require activities outside of the control room. There is no explicit discussion of this change, however. In addition, the term "hesitancy" has been changed to "burden" and includes additional factors. The following represents Dougherty and Fragola's example list of sources of burden:

- Time-constraint-related
  - one action with a short available time
  - multiple activities over a single duration
- Diagnosis-related
  - confusing indications
  - credibility of events

6

- complexity of events or systems
- Decision-making-related
    - planning or decision-making required
    - conflict between an option and a normal intention
    - competing resources
- Command and control-related
    - remoteness between people who need to communicate
    - remoteness of actions from the control room
    - distance between indications and controls
- Physiology-related
    - hostile environment.

The time/reliability correlations presented in [2] are based on a cumulative lognormal distribution, shown in its general form in equation 2.2:

$$HFP_p = \Phi\left[-\frac{\ln(t/m) - \sigma_\mu \Phi^{-1}(p)}{\sqrt{(\sigma_r^2 + \sigma_\mu^2)}}\right]$$

(2.2)

where:

HFP_p = human failure probability at the "p"th percentile

t = time available for response (time from initiator to core damage without the response *minus* the time to the critical symptoms *minus* the physical response time)

m = median time to respond

σ_r = lognormal standard deviation for data uncertainty

σ_μ = lognormal standard deviation for model uncertainty.

The authors of the method acknowledge directly that the time/reliability correlations are judgmental, and that there are no data sources that can be directly referenced for most of the parameters used in the above equation. The following is a summary of the rationale used to derive default or typical values for the parameters of median response times and the data and modeling uncertainties. The method's authors do state that users of the method can vary any of these values on the basis of their own judgments. However, the FCS IPE analyses have been based on the values discussed below.

Median Response Time. The value of the median time to respond is not discussed explicitly in [2]. However, the application presented in the FCS IPE discusses this parameter and its relationship to the different time/reliability correlations for verification, rule-based, and other response actions.

The "base-case" estimate from which other estimates of the median response time are derived is for the case of "other" response actions. This case, argue the authors, corresponds to the median human error probability (HEP) case of the nominal diagnosis time/reliability correlation modeled by Swain and Guttmann in Table 20-3 of [3]. From

7

that time/reliability correlation, a median response time of four minutes is derived as discussed in Table 10-2 of [2]. This analysis is performed by taking the failure probabilities presented in Table 20-3 associated with 10 and 20 minutes and fitting a lognormal distribution to intersect these points. Analyzing the resulting lognormal-distribution approximation of the Swain and Guttmann time/reliability correlation yields the median response time of 4 minutes. This value is used in the SAIC time/reliability correlations for "other" response actions.

In order to represent the response time for rule-based actions, Dougherty and Fragola observe that Swain and Guttmann recommend the use of the lower-bound HEP case of the time/reliability correlation in Figure 12-4 of [3] for situations where symptoms are clear and training is well understood and practiced in the simulator; this description also corresponds to the "rule-based" time/reliability correlation provided by Swain in the HRA method developed for the NRC's Accident Sequence Evaluation Program [4]. The median response time implicit in these time/reliability correlations is 2 minutes, which is used in SAIC's "rule-based" time/reliability correlations.

Using the rationale that the transition from the "other response" to the rule-based time/reliability correlations corresponds to a halving of the median response time, a further halving is used in the transition from rule-based actions to verification actions. That is, a median response time of 1 minute is used for the verification-action time/reliability correlations.

In the case of ex-control-room actions, the median response times are estimated on a case-by-case basis by plant operations personnel from their knowledge and experience or from walkdowns. The calculational process incorporates factors like the presence of steam or high radiation levels that can influence the time required to access certain areas of the plant by increasing the median response time by the estimated delay that such factors would cause.

In the SAIC method, two adjustments can be made in the median response time, to incorporate the effects of burden and to adjust for the influence of performance-shaping factors. The presence of burden is judged to have the effect of doubling the median response time used in the equation presented above. Similarly, the influence of the plant-specific performance-shaping factors can be modeled as an adjustment in the median response time, as discussed earlier.

The authors of the method observe that the range of time/reliability correlations generated by use of these median response times fall broadly in the ranges of time/reliability correlations generated from plant simulator data such as those cited in NUREG/CR-3010 [5].

Uncertainty Measures. The underlying equation for the SAIC time/reliability correlations involves two measures of uncertainty: those associated with data uncertainties, and those with modeling uncertainties. The derivation of the uncertainty measures is discussed in pages 119-129 of [2]; the following is a brief summary of the estimation process.

8

The estimate of data uncertainty is derived from the time/reliability correlation of Swain and Guttmann that underlay the estimation of the median response time of 4 minutes discussed above. Based on the calculations presented in Table 10-2 of [2], a generic, or default, value of 0.7071 is used for σ, in the in-control-room time/reliability correlations. A larger value, of 0.8994, is used for the ex-control-room cases, though no description of its derivation is provided.

In the case of responses judged to involve burden (discussed earlier), the data uncertainty value is increased consistent with a doubling in the error factor from which σ, has been derived.

The authors of the method concede that no data are available from which to derive modeling uncertainty estimates directly. A value of 0.315 is assigned to σ_u principally as a judgmental value on the basis that the resulting human error probabilities seem "reasonable".

Performance-Shaping Factors. Plant performance-shaping factors (PSFs) can be taken into account through parametric adjustments in the time/reliability correlations. The process of taking account of these factors involves the calculation of a success likelihood index (SLI) that represents an overall measure of the adequacy of such factors as the displays, procedures, and training, and the effectiveness of communications and teamwork. No unique set of PSFs are specified but the above factors are used in examples in [2],.

A SLI is a numerical index that represents the combined influence of a set of PSFs on the estimate of a human error probability. It was developed as part of an integrated human-reliability method called the Success Likelihood Index Method (SLIM) [6]. It is calculated by assessing a weight (representing how relatively important the particular PSF is to the human error probability) and a ranking (representing the "quality" of the particular PSF) for each PSF, and then summing across all of the PSFs.

However, in the FCS IPE application, it seems that a default neutral value was assigned by the analysts for the SLI value and, thus, no influence of any plant-specific PSFs was effectively incorporated in the results of these HRA studies. This lack of influence of plant-specific PSFs is considered a limitation in the FCS IPE.

2.1.1.3 Decision Tree. Dougherty and Fragola present a decision tree (Figure 9-1 of [2]) to identify which of the models should be applied for any particular human action; this decision tree is reproduced in Figure 2-1.

In the example applications, this decision tree appears to have been followed. In general, "plan-driven activities" refers to pre-initiator human actions in that there is no inherent time limitation by which actions must be completed. Within this category, "unspecifiable tasks" refers to situations that have not previously been planned, such as *ad-hoc* or novel repairs. No modeling of this category was performed in the FCS IPE.

In addition, no modeling of errors of commission associated with mistakes in the "event-driven activities" was performed in the FCS IPE. The confusion-matrix method identified in Figure 2-1 is a technique that allows an analyst to specify the likelihood of misdiagnosing some event "x" as event "y" based on such factors as the similarity of indications and alarms; it was developed by Potash for use in the Oconee PRA performed for the U.S. Nuclear Safety Analysis Center (NSAC) and is described in [7]. Since the U.S. nuclear industry's adoption of symptom-based emergency operating procedures, no PRA has used this method because of the perceived lack of need to model operators' errors in diagnosis.

2.1.1.4 Incorporation of human actions into the PRA Logic Models. Incorporation of human actions into the PRA models is described by Dougherty and Fragola as being performed by the systems-analysis task. Brief guidelines are provided in Chapter 9 of [2] for appropriate ways to incorporate human actions into PRA models. Specifically pre-initiator human actions are to be modeled in the system fault trees at the "highest" level consistent with the level of aggregation of the actions modeled (at the individual action step or for the task as a whole). The "highest level" is described as being typically at the train or part-train level of the system fault tree.

Post-initiator response human actions are to be modeled at the event-tree level, in the event "top logic" or at the highest level of the system fault trees. Post-initiator recovery human actions are to be added following initial sequence quantification to only those cut-sets that are significant contributors to the frequency of core damage; they are not added explicitly to the PRA logic models.

In addition to the pre-initiator and post-initiator human actions, Dougherty and Fragola recognize that human actions can act as initiating events. However, these are considered to be incorporated implicitly in the initiating-event frequencies, an assumption used in most PRAs. Therefore no separate modeling of initiating-event human actions is performed.

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

FCS is a single-unit station. Therefore there are no multi-unit effects.

The licensee has provided limited information concerning the activities to ensure that the IPE HRA analysis represents the as-built and as-operated unit. The following represent activities listed in the submittal to this end:

1) the use of experienced plant personnel, including one senior reactor operator (SRO), to compose the licensee's PRA group;

2) the use of plant information and plant walk-downs as the basis for the systems' analysis notebooks:

   • updated safety analysis report

   • technical specifications

10

- abnormal, emergency, and maintenance procedures, and plant operating instructions

- licensee event reports

- plant drawings and blue-prints

- training materials

- maintenance and surveillance data;

3) the reviews provided by plant staff and external reviewers.

However no specific information is provided as to how this information was used in the HRA task in particular.

2.1.3 Licensee Participation and Peer Review.

2.1.3.1 Licensee Participation. The HRA task was performed as part of the Level 1 PRA. The submittal identifies that the Level 1 PRA was largely performed by the licensee's PRA Group, which included plant personnel with 65 years of accumulated FCS plant experience and included the presence of a senior reactor operator (SRO). This work of this group involved extensive interfacing and review with personnel from the Licensee's Production Engineering Division, and operations, maintenance and reliability engineering personnel.

No explicit role of licensee personnel in the HRA task is described.

2.1.3.2 Peer Review. Three levels of review were provided for the IPE. The first level was provided by a PRA Oversight Committee staffed by licensee personnel from several departments including licensing, training and operations; this committee helped to ensure the technical accuracy of the models. The second level of review, provided by the PRA Executive Committee comprised of senior licensee management, was associated with reviewing any significant PRA findings and their resolution. The third level of review was provided by people external to the licensee, and was comprised of staff from Duke Engineering, Yankee Atomic Electric Company, and ABB/Combustion Engineering.

The HRA analyses are identified as being reviewed by all three levels, though no issues associated with the HRA task are identified in the discussion of comments.

2.2 Pre-Initiator Human Actions

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

11

multiple actions.

Within the categorization of errors discussed in Section 2.1.1, all pre-initiator human actions were modeled as slips.

2.2.1   Types of Pre-Initiator Human Actions Considered.

The licensee included consideration of:

1)   failures of plant personnel to restore components and systems following testing and maintenance, and

2)   failures during calibration of instrumentation and control equipment.

These failures represent an appropriate range of pre-initiator human actions.

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

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

No explicit description of the process for the initial identification of pre-initiator human actions is provided. However the following is inferred from the description of the fault trees' development and the description of information used in the IPE.

First, systems that could influence the development of accident sequences were identified and selected as part of the front-end analysis. For each such system, detailed systems' analysis notebooks were prepared. These included identification of all components whose states were changed during testing and maintenance, as defined in the FCS test and maintenance procedures. Those components whose changes of state during testing and maintenance could lead to system or train failures (within the definition of the system fault trees) were then reviewed using a qualitative screening process to identify those pre-initiator human actions to be subject to detailed HRA quantification modeling. The screening process and the detailed quantification process are described in the following sections.

The review process summarized in Section 2.1.3 included reviews by plant personnel (including operations, training, and maintenance departments) that should have ensured the correctness of interpretation and implementation of the plant's test, maintenance and calibration procedures.

It is concluded that the process for identification and selection of pre-initiator human actions was appropriate and adequate for the purpose of the analysis.

2.2.3 Screening Process for Pre-Initiator Human Actions.

The licensee applied the screening process associated with slips described in Section 2.1.1.1 to the pre-initiator human actions. Following the screening analysis, 17 pre-initiator human actions were identified for detailed modeling.

It is unclear whether the screening values used for pre-initiator human actions will identify all potentially significant human actions for detailed analysis. The basic value, of 0.003, is not significantly greater than the failure probabilities estimated from actual failures reported in event reports and the plant-specific failure data.

In those cases where the plant-specific data includes human-related causes, the separate modeling of human causes for the same components is unnecessary and would result in double-counting – one of the licensee's stated reasons for using a low screening value. However, the components that include plant-specific data are limited mostly to major electro-mechanical devices like pumps and valves; for example, no plant data are used for instrumentation failure rates presented in Table 3.3.1. Therefore it is possible that components for which the plant-specific experience is poor to be excluded from the detailed analysis through the use of the low generic screening value that leads to the related accident cut-sets being lower than the PRA cut-off value for detailed modeling.

The potential for excluding components that have poor plant-specific performance through the use of a low screening value is considered a limitation in the FCS IPE.

2.2.4 Quantification Process for Pre-Initiator Human Actions.

The licensee applied the detailed quantification process associated with slips, described in Section 2.1.1.2, to the 17 pre-initiator human actions identified in the screening analysis. A complete list of these 17 pre-initiator human actions, with their estimated failure probabilities is presented in Table 4-1.

Of the 17, two were identified through the sensitivity analysis as having the potential for contributing significantly to the core-damage frequency. (The sensitivity analysis is described in Section 2.4.2.) These are:

1) GHFLPRESS – Human miscalibrates Safety Injection Refueling Water Tank (SIRWT) level pressure switches and transfer to recirculation occurs too soon; failure probability = 3.0E-04;

2) KJUMPER – Failure to remove RPS interposing relay jumpers prior to power operations; failure probability = 1.3E-06.

The modeling of both human actions included the effects of dependencies associated with multiple trains and interpersonal dependencies identified in Equation 2.1 in Section 2.1.1.2.

In addition, the FCS IPE included an analysis of Fussel-Vesely importance measures. (The importance analysis is discussed in section 2.4.2.) No pre-initiator human actions were identified as being identified as significant by the importance-measures analysis.

As described in Section 2.1.1.2, the detailed quantification of pre-initiator human actions is performed using a very simplistic model. The model as applied in the FCS IPE would seem not to include any analysis of plant-specific human-system factors like the layout of controls, the use of labeling, or the formatting of procedures.

The use of the simplistic quantification model, and particularly the exclusion of any consideration of plant-specific human-system factors, in the detailed quantification of pre-initiator human actions is considered a limitation in the FCS IPE.

2.3   Post-Initiator Human Actions

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

2.3.1   Types of Post-Initiator Human Actions.

The analysis of post-initiator human actions included the modeling of both slips and mistakes using the models described in Section 2.1.1. A limited number of actions are associated with internal floods and one action is associated with preserving the integrity of the containment in the post-core-damage phase of the accident.

The licensee does not describe the logic applied to decide which post-initiator actions should be modeled as slips and which as mistakes. Figure 2-1 identifies the selection of an appropriate model for quantifying slips and mistakes, but does not describe the choice between a slip and a mistake for any particular action. Since using the different models can lead to significantly different probabilities of failure, the lack of guidance as to whether to select an action as a slip or a mistake is a potential limitation in the method and in the IPE.

Two operator-related modifications were identified as a result of performing the IPE. These were:

2)   the addition of a manually closed door to permit access to isolate the component-cooling water system in the event of flooding from failure of a reactor coolant pump (RCP) seal cooler; and

2)   modification of the procedure for responding to alarms associated with

14

flooding in the safety-injection (SI) and containment-spray (CS) pump rooms, directing operators to open the water-tight door (No. 971-1 in Room 23) to allow drainage of the water from the rooms or closed for floods initiating in Room 23.

The submittal shows modification 1 as being complete and modification 2 in progress.

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 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.

As in the case of the pre-initiator human actions, the licensee provides no explicit descriptions of the process used to identify post-initiator human actions for analysis. However, data sources used to identify these actions included the emergency and abnormal operating procedures (EOPs and AOPs), walk-downs of the plant and control facilities, and discussions with appropriate plant personnel. It is noted that the licensee's HRA team did include a senior reactor operator.

All post-initiator human actions were incorporated into the plant logic models with the joint agreement of the systems analysts and the HRA analysts.

The submittal identifies that some non-proceduralized actions were identified and modeled in the HRA analysis. When such actions were discovered, appropriate changes to procedures were identified and the modeling took into account these actions with a suitable "reliability decrement" through the use of the appropriate time/reliability correlations discussed in Section 2.1.1.

2.3.3 Screening Process for Post-Initiator Human Actions.

Separate screening processes were used for slips and mistakes in the analysis of post-initiator human actions. In the case of slips, a single failure probability of 1.0 was assigned as the screening value, and a single failure probability of 0.4 was assigned for mistakes. These probabilities are considered suitable values for screening purposes.

As a result, 19 post-initiator slips and 25 mistakes were identified for detailed modeling.

2.3.4 Quantification Process for Post-Initiator Human Actions.

2.3.4.1 Detailed Quantification of Slips. The 19 slips identified from the screening analysis were quantified using the detailed quantification model described by Equation 2-

1 in Section 2.1.1.1. A complete list of these 19 slips, with their estimated failure probabilities, is presented in Table 4-1.

Of the 19 post-initiator slips, five were identified in sensitivity analysis as having the potential for providing a significant contribution to the core-damage frequency. These are:

1) OPER-41 – failure to make up to the emergency feedwater storage tank (EFWST) with the diesel-driven auxiliary feedwater pump; failure probability = 5.3E-04;

2) OPER-70 – failure to depressurize the reactor coolant system (RCS) in response to an interfacing systems loss-off-coolant accident (ISLOCA); failure probability = 2.1E-04;

3) EHFFEOP-00 – failure to reload equipment (such as air compressors) following loss-of-offsite power, as required in post-trip procedure EOP-00; failure probability = 3.0E-03;

4) OPER-9 – failure to depressurize and terminate RCS primary-secondary leakage following a steam-generator tube rupture (SGTR); failure probability = 2.1E-04; and

5) AHFFCONTROL – failure to control auxiliary feedwater (AFW) flow and prevent flooding of the steam-driven AFW pump; failure probability = 1.0E-03.

In addition, the importance-measure analysis identified one post-initiator slip as having the third-highest Fussel-Vesely importance measure; this is event OPER-41 described above.

As discussed with regard to the analysis of pre-accident human actions, the model used to quantify post-initiator slips is very simplistic and takes no account of the plant-specific factors associated with these human actions. The use of this simplistic model lacking the incorporation of plant-specific factors is considered a limitation in the FCS IPE.

In addition, the selection of post-initiator actions as slips is not always clear. For example, it is not clear why some of the actions identified above, such as OPER-9 and OPER-71, are considered to be slips. Both OPER-9 and -71 would seem to involve significant diagnostic and decision-making activities, and be time-limited to prevent core damage; these are characteristics more often associated with mistakes. However, the licensee has provided some general guidance as to when consider actions as slips or mistakes. In general, the HRA analyst must apply judgment as to whether there is a greater likelihood of a mistake or a slip depending on the complexity of the event and the complexity and quality of the interface.

2.3.4.2 Detailed Quantification of Mistakes. The 25 mistakes identified in the screening analysis were quantified using the model described by Equation 2-2 in Section 2.1.1.2. A

16

list of these 25 mistakes, with their estimated failure probabilities, is presented in Table 4-1.

Two post-initiator mistakes were identified in the sensitivity analysis as having the potential to significantly affect the core-damage frequency. These are:

1) AHFFEFWST – failure to align makeup flow to the EFWST from any source (ex-control room); failure probability = 3.0E-03; and

2) OPER-4 – failure to initiate feed-and-bleed when required (rule-based, in control room); failure probability = 2.3E-03.

In addition, two post-initiator mistakes were identified by the importance analysis as having the sixth- and eighth-highest Fussel-Vesely importance measure. These were respectively:

- XEFWST – failure to use diesel-driven fire pump to replenish the EFWST (ex-control room); failure probability = 7.8E-02; and

- XBRKRTRIP – failure to manually trip 4160 VAC breaker given the breaker failed to trip automatically (rule-based, in control room); failure probability = 0.15.

2.3.5 Generic Issues and Containment Performance Improvement.

2.3.5.1 Decay Heat Removal. The licensee recognizes that human actions play an important role in preventing core damage from failures in the decay-heat-removal process. Two sets of actions are identified: those to ensure that long-term heat removal via the steam generators can be maintained by refilling the EFWST, and feed-and-bleed cooling if secondary-side cooling is lost. The licensee has identified several means for the operators to replenish the inventory of the EFWST, including use of the fire-pump hook-up. The failure to line up flow to the EFWST within 8 hours involves actions outside of the control room is estimated to have a failure probability of 3.0E-03 (event AHFFEFWST).

Sequence "TX", a transient initiating event with failure of long-term cooling (via shutdown cooling or long-term make-up to the EFWST if main feed water is not available), is the largest contributing functional sequence to the FCS core-damage frequency, comprising 39%, or 5.3E-06 per year. No breakdown of the human contributions to this sequence are reported.

Feed-and-bleed cooling is described as being included in the FCS EOPs and requires operation of only one power-operated relief valve (PORV) and one high-pressure safety-injection (SI) pump. Initiation of feed-and-bleed cooling can be performed from within the control room. Failure to initiate feed-and-bleed cooling following a transient is estimated to have a failure probability of 2.3E-03 (events OPER-4 and OPER-4E).

17

Functional sequence "TBF", a transient initiating event with failures of secondary cooling and feed-and-bleed cooling, comprises the third largest sequence, comprising 10.6% of the FCS internal-events core-damage frequency, or 1.5E-06 per year. . No breakdown of the human contributions to this sequence are reported.

2.3.5.2 Containment Performance Improvements. No human actions are identified in relation to containment performance improvements.

2.3.6 Internal Flooding.

A total of nine human actions are associated with the modeling of internal flooding. Eight of the nine actions are events already identified in the internal-events analysis, and one new event unique to the internal-flooding analysis was identified. Table 2-3 summarizes these nine events.

Most of the dominant internal-flood sequences include combinations of human actions listed in Table 2-3, but no details of the relative contributions of these actions to the frequency of core damage from internal floods are provided. However, the submittal does identify that events WHFFRWBKUP and XSIRWT are "key contributors."

In addition, one plant improvement associated with internal floods was identified. This is a modification of the procedure for responding to alarms associated with flooding in the safety-injection (SI) and containment-spray (CS) pump rooms, directing operators to open the water-tight door (No. 971-1 in Room 23) to allow drainage of the water from the rooms or to close the door for floods initiating in Room 23. The submittal shows the modification to be in progress.

2.4   Vulnerabilities, Insights, and Enhancements

2.4.1 Vulnerabilities.

The licensee applied the criteria from NUMARC 91-04 as the basis for screening plant-specific vulnerabilities. Based on these criteria, three functional accident sequences were identified as having core-damage frequencies within the range 1E-5 to 1E-6 per year. These are:

1)   TX – transient initiating event with failure of long-term heat removal;

2)   TQ2U – transient-induced RCP seal LOCA with failure of high-pressure safety injection; and

3)   TBF – transient initiating event followed by failures of primary-secondary heat removal and feed-and-bleed cooling.

Functional sequences TX and TBF involve human actions; initiating long-term heat removal and replenishing the EFWST in sequence TX, and establishing feed-and-bleed cooling in sequence TBF.

Table 2-3. Summary of human actions in internal flooding analysis.

Event	Description	Internal-events HFP	Flooding HFP	Basis
EHFFEOP-02	Loss of offsite power and failure to reload bus 1C3A, per EOP-2	3.0E-02	3.0E-01	Entry into flooded area hampers recovery
EHFMBATTLD	Operator fails to minimize DC loads on batteries #1 and #2.	2.1E-03	1.0	Entry into flooded area judged unlikely
IHFFCA1C	Operator fails to start compressor CA1C	1.1E-05	1.0	Entry into flooded area judged unlikely
KHU56AC	Operator fails to reload HVAC to Room 56/56A given inverter fails	9.1E-03	1.0	Entry into flooded switchgear area not possible
KHUSI	Operator fails to shed SI loads and cool switchgear rooms after safeguards actuation	9.0E-03	1.0	Entry into flooded switchgear area not possible
OPER-10	Failure to achieve shutdown cooling	2.1E-02	2.1E-01	Entry into flooded area hampers recovery
WHFFRWBKUP	Failure to line up RW backup flow	7.2E-04	7.2E-03	Entry into flooded area hampers recovery
XFIREPUMP	Failure to align fire pump to CCW heat exchangers	7.0E-03	7.0E-02	Entry into flooded area hampers recovery
XSIRWT	Failure to make up to SIRWT after RAS failure occurs	Not used	1.0E-01	Screening value. Entry into flooded area not required.

The licensee states that severe accident management guidelines (SAMGs) will be developed for these functional sequences to prevent or mitigate core damage, vessel failure, or containment failure, in accordance with the NUMARC guidance.

2.4.2 Insights Related to Human Performance.

The licensee performed two analyses to identify insights associated with the risks of core damage at FCS. These were an analysis of Fussel-Vesely importances of basic events and a set of sensitivity analyses. One of the sensitivity analyses was an evaluation of human actions.

2.4.2.1 Importance Analysis. The licensee calculated Fussel-Vesely importance measures for the basic events in the Level 1 PRA models. Eight events were identified as

significant contributors to the core damage frequency, based on the importance measures. (The Fussel-Vesely importance measure of an event is a measure of what would be the reduction in core-damage frequency [CDF] if the failure probability of that event were zero.) Of these eight, three were post-initiator human actions:

- OPER-41 – failure to make up to the emergency feedwater storage tank (EFWST) with the diesel-driven auxiliary feedwater pump (slip); failure probability = 5.3E-04; change in FCS CDF = 25%;

- XE: WST B failure to use diesel-driven fire pump to replenish the EFWST (ex-control room mistake); failure probability = 7.8E-02; change in FCS CDF = 16%; and

- XBRKRTRIP B failure to manually trip 4160 VAC breaker given the breaker failed to trip automatically (rule-based mistake in control room); failure probability = 0.15; change in FCS CDF = 10%.

No pre-initiator human actions were identified in the importance analysis as being significant.

2.4.2.2 Sensitivity Analysis. A sensitivity analysis of pre- and post-initiator human actions was performed. The analysis was performed by setting the failure probability of each human action to 0.1 and calculating the resultant change in the FCS CDF. Based on this analysis, nine events were identified as having the potential to influence the CDF significantly. Two events were pre-initiator human actions. These are:

- GHFLPRESS – miscalibration of Safety Injection Refueling Water Tank (SIRWT) level pressure switches (causes transfer to recirculation too soon); failure probability = 3 JE-04; approximate increase in CDF = 5.2;

- KJUMPER – failure to remove RPS interposing relay jumpers prior to power operations; failure probability = 1.3E-06; approximate increase in CDF = 3.3.

The remaining seven events were post-initiator human actions:

- OPER-41 – failure to make up to the emergency feedwater storage tank (EFWST) with the diesel-driven auxiliary feedwater pump; failure probability = 5.3E-04; approximate increase in CDF = 4.7;

- AHFFEFWST – failure to align makeup flow to the EFWST from any source (ex-control room); failure probability = 3.0E-03; approximate increase in CDF = 3.3;

- OPER-4 – failure to initiate feed-and-bleed when required (rule-based, in control room); failure probability = 2.3E-03; approximate increase in CDF = 3.2.

- OPER-70 – failure to depressurize the reactor coolant system (RCS) in response to an interfacing systems loss-off-coolant accident (ISLOCA); failure probability = 2.1E-04; approximate increase in CDF = 3.1;

- EHFFEOP-00 – failure to reload equipment (such as air compressors) following loss-of-offsite power, as required in post-trip procedure EOP-00; failure probability = 3.0E-03; approximate increase in CDF = 2.6;

- OPER-9 – failure to depressurize and terminate RCS primary-secondary leakage following a steam-generator tube rupture (SGTR); failure probability = 2.1E-04; approximate increase in CDF = 1.8; and

- AHFFCONTROL – failure to control auxiliary feedwater (AFW) flow and prevent flooding of the steam-driven AFW pump; failure probability = 1.0E-03; approximate increase in CDF = 1.6.

The sensitivity analysis indicates that all other human actions increased the CDF by less than 1.25.

2.4.3 Human Performance-Related Enhancements.

Two operator-related enhancements were identified as a result of performing the IPE. These were:

1) the addition of a manually closed door to permit access to isolate the component-cooling water system in the event of flooding from failure of a reactor coolant pump (RCP) seal cooler; and

2) modification of the procedure for responding to alarms associated with flooding in the safety-injection (SI) and containment-spray (CS) pump rooms, directing operators to open the water-tight door (No. 971-1 in Room 23) to allow drainage of the water from the rooms, or to close the door for floods initiating in Room 23. (The door is normally open.)

The FCS submittal shows modification 1 as being complete and modification 2 in progress. The effect of modification 1 was credited in the IPE models. The internal-flooding analysis was performed assuming that the door in modification 2 was open.

21

Figure 2-1. Decision tree for selection of model.

Environs	Preparation	Mode	Effect	Technique
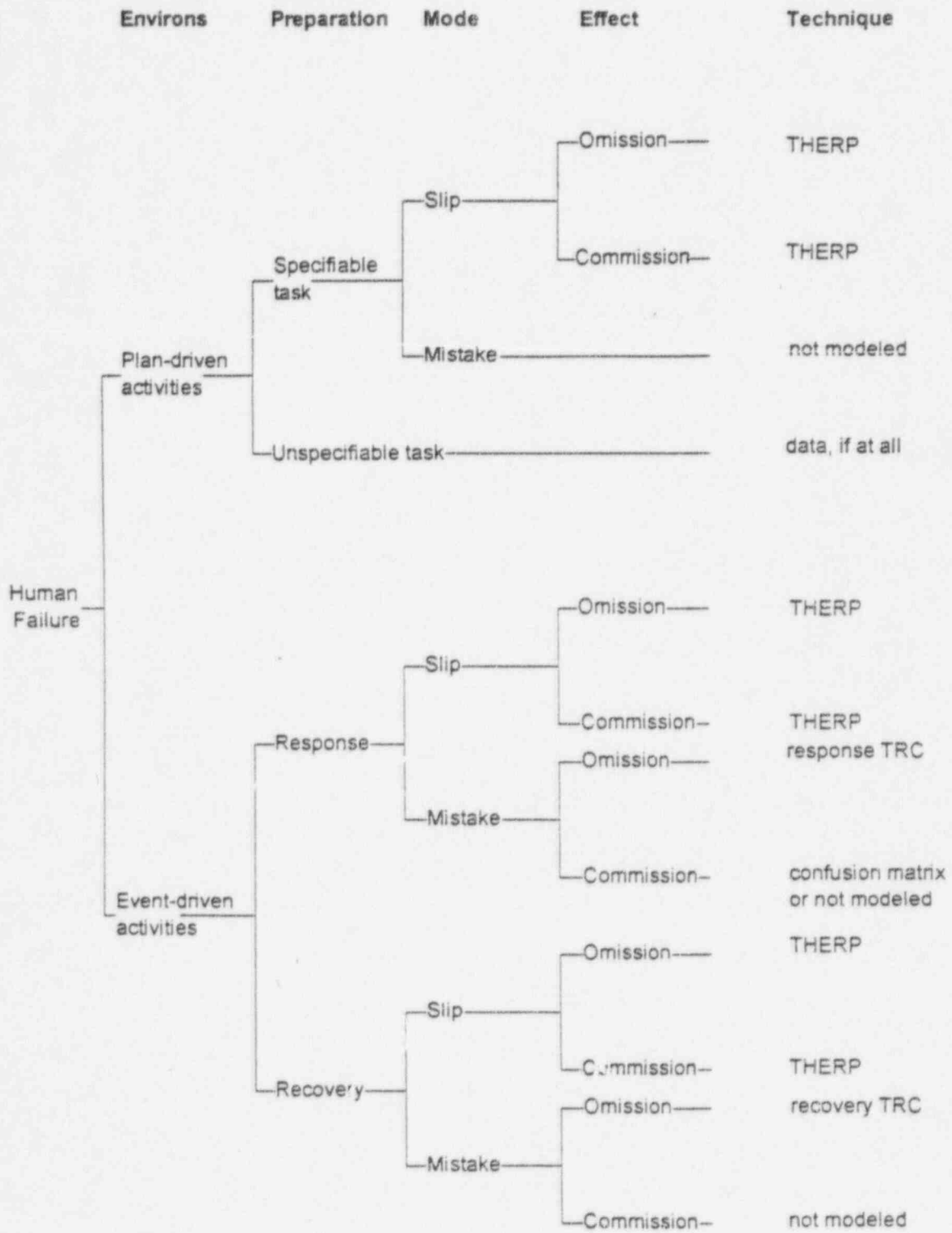
3.   CONTRACTOR OBSERVATIONS AND CONCLUSIONS

The intent of our document-only review of the licensee's HRA process and results is to determine whether the process supports the licensee's meeting specific objectives of GL 88-20 as they relate to human performance issues. That is, does the HRA process permits the licensee to:

1)   Develop an overall appreciation of human performance in severe accidents; how human actions can impact positively or negatively the course of severe accidents, and what factors influence human performance.

2)   Identify and understand the operator actions important to the most likely accident sequences and the impact of operator action in those sequences; understand how human actions affect or help determine which sequences are important.

3)   Gain a more quantitative understanding of the quantitative impact of human performance on the overall probability of core damage and radioactive material release.

4)   Identify potential vulnerabilities and enhancements, and if appropriate, implement reasonable human-performance related enhancements.

It is our general conclusion from the review of the submittal and the additional material provided by the licensee in response to NRC requests for additional information that the licensee's HRA process appears generally capable of providing the licensee with a general appreciation of the impact of human performance on the overall probabilities of core damage and fission-product releases.

However, there does not appear to be a thorough case-by-case (plant-specific and event-specific) assessment of some of the factors influencing human actions to assure a completely realistic understanding of human performance in the plant. The analysis of pre- and post-initiator human actions does not include any consideration of the human-system interface or the formatting of procedures, for example.

In addition, the quantification model used for slips contains weaknesses that may result in the under-estimation of the failure probabilities of both pre- and post-initiator human actions. In particular, the use of relatively low screening probabilities for pre-initiator slips could potentially lead to the omission of important actions from the detailed analyses. Additionally, the use of the simple model for the detailed analysis of slips (Equation 2.2) could lead to the under-estimation of probabilities of failure for components that have plant-specific weaknesses associated with the human-system interface.

There are some characteristics associated with the modeling of mistakes that can lead to seemingly inconsistent results. The model uses different time/reliability correlations depending on whether actions are verification, rule-based, or "other" actions, whether they occur inside or outside the control room, and whether the operators are burdened.

Differences in the quantification results based on different assumptions can be significant. Consider first the action to initiate feed-and-bleed cooling. In most cases, this action is to be performed within about 50 minutes, is rule-based, and is performed from the control room. The resulting probability of failure is typically 2.3E-03 (for example, events OPER-4 and OPER-8RB). However, in the event of a small LOCA the same action is assumed to be not burdened; since a breach in the vessel exists, the operator is not reluctant to create a new "breach". With no changes to the model other than removing the burden factor, the failure probability drops to 9.1E-06 (OPER-8). Some guidance is provided by the licensee as to when the burden factor should be incorporated but this guidance relies on the skill of the analyst.

In addition, the ex-control room time/reliability correlation leads to an estimated failure to accomplish long-term heat removal within 8 hours, of 2.1E-02 (event OPER-10). This probability, when compared with the reliability of other actions (for example, the feed-and-bleed actions just described) is considered disproportionately high. It is possible that this failure is one main reason why sequences initiated by transients and involving failure to accomplish long-term heat removal (the TX sequences) comprise such a large contribution (39%) to the frequency of core damage at FCS.

Other general observations include the following:

1) The method used in the FCS IPE does include explicit guidelines for the selection of models to be used in the quantification of human actions through the use of a decision tree. In addition, the submittal does describe how the human actions should be incorporated into the PRA logic models explicitly. Both of these features are considered strengths of the FCS IPE.

2) Some guidance is provided as to which actions should be modeled as slips or mistakes, but skilled judgments by the analyst are required. This demand could lead to limitations in future revisions of the FCS IPE if the analysts performing those revisions are not familiar with the judgments required in the analysis. However, the guidelines provided by the licensee appear reasonable in themselves.

3) In common with other time-based quantification methods, the FCS HRA modeling does not include consideration of one significant source of uncertainty in the quantification of mistakes: uncertainties in the estimation of the time available for action. While the estimation of the time available is described as not part of the HRA task, this is a critical input parameter to the HRA model and therefore it must be seen as a significant source of uncertainty for the HRA time-based models.

4) One human action was identified as part of the containment-performance analysis (event SPRAYRECOV). This action is to start manually containment sprays following their failure to initiate automatically following vessel breach. The licensee assigned a failure probability of 0.0 to this action. While this probability is clearly optimistic for actions taken

during the "heat of battle" following vessel failure, the licensee claims that the impact of any optimism is not significant.

5) Several human actions were incorporated explicitly in the modeling of internal floods. In those cases where the actions were similar to those represented in the internal-events analysis, the probabilities were adjusted judgmentally to allow for the delays or impossibility of access to equipment. One action was identified as being unique to the flooding analysis.

6) This IPE is unique in that a limited number of potentially significant errors of commission were identified that have the potential to create new accident scenarios. Examples include:

- OPER-11X – Operator prematurely closes PORVs after initiating feed-and-bleed;

- OPER-12SX – Operator fails long-term cooling (SG cooling available, SLOCA); and

- OPER-20 – Operator fails high-pressure recirculation during small-break LOCA, without SG cooling.

These events are not quantified and therefore do not impact the FCS risk parameters. The submittal provides no discussion of the identification or possible significance of these actions. However, this is one of the very few PRAs (and perhaps the only IPE) to have even considered the possibility of operators performing inappropriate actions that create new accident scenarios.

4.   PLANT DATA

4.1   Important Operator Actions.

Several of the dominant accident sequences in the FCS IPE include significant contributions from human errors. These include:

- TX – transient initiating event with failure of long-term heat removal (39% of FCS CDF);

- TBF – transient initiating event followed by failures of primary-secondary heat removal and feed-and-bleed cooling (11% of CDF);

- RX - steam-generator tube rupture with failure of long-term heat removal and inventory make-up (4.5% of CDF).

Sequences TX and RX include failures of human actions to ensure long-term heat removal (and inventory make-up for RX). Sequence TBF includes failures of human actions to ensure feed-and-bleed cooling.

The Fussel-Vesely importance analysis identified three human actions as being significant:

- OPER-41 – failure to make up to the emergency feedwater storage tank (EFWST) with the diesel-driven auxiliary feedwater pump;

- XEFWST – failure to use diesel-driven fire pump to replenish the EFWST; and

- XBRKRTRIP – failure to manually trip 4160 VAC breaker given the breaker failed to trip automatically.

Table 4-1 summarizes the human actions events analyzed in the FCS IPE. In those cases where the same action is used in the internal-events and internal-flooding analyses, the failure probability is cited for the internal-events analysis. Corresponding values for the internal-flooding analysis are presented in Table 2-3.

4.2   Human Performance-Related Enhancements

Two operator-related enhancements were identified as a result of performing the IPE. These were:

1)   the addition of a manually closed door to permit access to isolate the component-cooling water system in the event of flooding from failure of a reactor coolant pump (RCP) seal cooler; and

2)   modification of the procedure for responding to alarms associated with flooding in the safety-injection (SI) and containment-spray (CS) pump rooms, directing operators to open the water-tight door (No. 971-1 in Room 23) to allow drainage of the water from the rooms, or to close the door for floods initiating in Room 23. (The door is normally open.)

The FCS submittal shows modification 1 as being complete and modification 2 in progress. The effect of modification 1 was credited in the IPE models. The internal-flooding analysis was performed assuming that the door in modification 2 was open.

Table 4-1. Human actions events analyzed in the FCS IPE.

Event	Action	Error Probability
AHFCONTROL	Operator fails to control AFW to SGs given HCV-1107 or 1108 fails open	1.0e-03
AHFFEFWST	Failure to line up make-up flow to the EFWST within 8 hours	3.0e-03
AHFFLEVEL	Failure to align flow to EFWST given instrumentation failure	1.2e-03
BHFLSITRPS	CCF of the SI tanks due to pressure transmitter miscalibration	3.0e-04
EHFFEOP-00	Operator fails to reload equipment per EOP-00 following loss-of-offsite power	3.0e-03
EHFFEOP-02	Loss-of-offsite power and human failure to reload bus 1C3A per EOP-02	3.0e-02
EHFM143SD1	Switch 143/SS on control panel D1 left in "local maintenance" position	3.0e-03
EHFM143SD2	Switch 143/SS on control panel D2 left in "local maintenance" position	3.0e-03
EHFM1A11A3	Control switch 43-Auto/1A1-1A3 not in auto	3.0e-03
EHFM1A11A4	Control switch 43-Auto/1A2-1A4 not in auto	3.0e-03
EHFM43-1D1	Diesel Gen. mode switch 43-1/1AD1 left in off-auto position following testing	3.0e-03
EHFM43-1D2	Diesel Gen. mode switch 43-1/1AD2 left in off-auto position following testing	3.0e-03
EHFMBATTLD	Operator fails to minimize DC loads on batteries #1 and #2	2.1e-03
GHFC00AFAS	Miscalibration of the AFAS level and pressure sensors	3.0e-04
GHFC00CPHS	Miscalibration of the CPHS pressure sensors	3.0e-04
GHFC00STLS	Miscalibration of the STLS level sensors such that RAS does not initiate	3.0e-04
GHFLPRESS	Miscalibration of the SIRWT level pressure sensors (STLS occurs too soon)	3.0e-04
HHFFHCLI	Operator fails to establish HCLI	6.0e-05
HHFLSI111	SI-111 left closed after maintenance	3.0e-03
HHFLSI112	Drain valve left closed after maintenance	3.0e-03
IHFFCA1C	Operator fails to start compressor CA-1C	1.1e-05
IHFLAC1035	Intercooler outlet valve AC-1035 left open after maintenance	3.0e-03

27

Event	Action	Error Probability
IHFLAC1039	Intercooler outlet valve AC-1039 left open after maintenance	3.0e-03
KJUMPER	Failure to remove RPS interposing relay jumpers prior to power operations	1.3e-06
KHU56AC	Operator fails to reload HVAC to room 56/56A, given interverter fails	9.2e-03
KHU56ACINV	Operator fails to reload HVAC to room 56/56A, prior to loss of interverter	9.2e-03
KHUSI	Operator fails to shed SI loads and cool switchgear rooms after SI signal	9.0e-03
LHFFSTARTR	Failure to restart LPSI pump after RAS	1.0e+00
OPER-4	Failure to initiate feed-and-bleed (transients except T4)	2.3e-03
OPER-4E	Failure to initiate feed-and-bleed (RX and TX)	2.3e-02
OPER-5	Failure to initiate shutdown cooling	2.1e-02
OPER-6	Operator fails long-term cooling/inventory control (RQX - SIWRT may be only option)	2.8e-03
OPER-8	Failure to initiate feed-and-bleed during SLOCA	9.1e-06
OPER-8RB	Failure to initiate feed-and-bleed during SGTR	2.3e-03
OPER-9	Operator fails to terminate faulted SG leakage	2.1e-04
OPER-10	Failure to achieve shutdown cooling	2.1e-02
OPER-11X	Operator prematurely closes PORVs after feed-and-bleed	0.0e+00
OPER-12SX	Operator fails long-term cooling (SG cooling available-SLOCA)	0.0e+00
OPER-13	Operator fails SD cooling & HP recirculation after feed-and-bleed	0.0e+00
OPER-20	Operator fails HPR during SLOCA w/o SG cooling	0.0e+00
OPER-23	Operator fails to isolate opened PORV path	2.1e-04
OPER-24	Operator fails to feed/steam SGs for long-term decay-heat removal	0.0e+00
OPER-35	Operator fails to close block valves HCV-150 or -151 (See OPER-23)	2.1e-04
OPER-40	Operator fails to provide flow to SGs from AFW FW-54	3.2e-04
OPER-41	Operator fails to use FW-54 for make-up to EFWST	5.3e-04
OPER-50	Operator fails to initiate emergency boron	3.0e-03
OPER-60	Operator fails to isolate ISLOCA leak by closing HCV-438B or -438D from control room	1.5e-03
OPER-65	Operator fails to isolate ISLOCA leak by hand-jacking HCV-438D closed	1.6e-04
OPER-70	Operator fails to depressurize RCS in response to ISLOCA	2.1e-04
OPER-71	Operator fails to depressurize RCS to atmospheric pressure in response to ISLOCA	1.0e+00
OPER-101	Operator fails to achieve shutdown cooling (ISLOCA)	7.2e-04
SHFFCW-6A	Operator fails to line-up bearing water cooler CW-6A	3.4e-01
SHFFMISCLA	Operator miscalibrates temperature controller TCV-1919A	3.0e-04
SIRWRM4	Operator fails to make-up to SIRWT (all SIRWT water flows out of rupture)	7.9e-03

Event	Action	Error Probability
SPRAYRECOV	Operator fails to manually recover containment-spray system following vessel breach (CS available)	0.0e+00
WHFFRWBKUP	Operator fails to line up RW backup flow	7.2e-04
XAFWSTART	Operator fails to manually initiate AFW	1.1e-04
XBACKFEEDA	Operator fails to align 345kV backfeed prior to core damage (AU and M events)	7.0e-02
XBACKFEEDS	Operator fails to align 345kV backfeed prior to core damage (R, S, T events)	2.8e-02
XBACKFEEDX	Operator fails to align 345kV backfeed and make-up to EFWST	1.4e-04
XBADRAS	Operator fails to realign SI pump suction to SIRWT prior to loss of pump suction	1.0e-01
XBRKRTRIP	Operator fails to manually trip 4160V breaker	1.5e-01
XCHARGER3	Operator fails to align spare battery charger #3 to DC bus	4.2e-02
XDGREMOTE	Operator fails to start DG from control room after auto start, and prior to EFWST empties	4.2e-04
XEFWST	Operator fails to provide make-up to EFWST via fire-pump hookup	7.8e-02
XFEEDRING	Operator fails to align aux. feed to S/G via main feed ring	1.1e-04
XFIREPUMP	Operator fails to align fire pump to CCW heat exchangers	7.0e-03
XMANRAS	Operator fails to manually initiate RAS prior to loss of pump suction	3.0e-02
XMANTRIP	Operator fails to trip reactor manually	0.0e+00
XSIRWT	Operator fails to make up to SIRWT after RAS failure (internal flooding)	1.0e+00
X161KV	Operator fails to align 161kV manually after fast transfer fails	5.9e-05

5.   REFERENCES

[1]   J. Reason and K. Mycielska, *Absent-Minded? The Psychology of Mental Lapses and Everyday Errors*. Englewood Cliffs, NJ: Prentice-Hall, 1982.

[2]   E. M. Dougherty, Jr. and J. R. Fragola, *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications*. New York: John Wiley & Sons, Inc., 1988.

[3]   A. D. Swain and H. E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, Sandia National Laboratories, Albuquerque, NM, NUREG/CR-1278, Rev. 1, August 1983.

[4]   A. D. Swain, *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*, Sandia National Laboratories, Albuquerque, NM, NUREG/CR-4772, February 1987.

[5]   R. E. Hall, J. R. Fragola, and J. Wreathall, *Post-Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation*, Brookhaven National Laboratory, Upton, NY, NUREG/CR-3010, November 1982.

[6]   D. E. Embrey, P. Humphreys, E. A. Rosa, B. Kirwan, and K. Rea, *SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment (Vols. I & II)*, Brookhaven National Laboratory, Upton, NY, NUREG/CR-3518, 1984.

[7]   L. M. Potash, M. Stewart, P. E. Dietz, D. M. Lewis, and E. M. Dougherty, Jr, *Experience in integrating the operator contribution in the PRA of actual operating plants*, presented at ANS/ENS Topical Meeting on Probabilistic Risk Assessment, Port Chester, NY, 1981.

APPENDIX C

BACK-END (CONTAINMENT) TECHNICAL EVALUATION REPORT