

CONCORD ASSOCIATES, INC.

Systems Performance Engineers

CA/TR 96-019-45

**WOLF CREEK GENERATING
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.
Herndon, VA 22070
(703) 318-9262

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

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

11-21-96

9609300310

XA

WOLF CREEK GENERATING 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

CONCORD ASSOCIATES, INC.
Systems Performance Engineers

725 Pellissippi Parkway
Knoxville, TN 37932

Contract No. NRC-04-91-069
Task Order No. 45

TABLE OF CONTENTS

E.	EXECUTIVE SUMMARY	E1
E1.	Plant Characterization	E1
E2.	Licensee IPE Process	E1
E3.	Human Reliability Analysis	E1
E4.	Generic Issues and CPI	E6
E5.	Vulnerabilities and Plant Improvements	E6
E6.	Observations	E8
1.	INTRODUCTION	1
1.1	Review Process	1
1.2	Plant Characterization	1
2.	TECHNICAL REVIEW	2
2.1	Licensee IPE Process	2
2.1.1	Completeness and Methodology	2
2.1.2	Multi-Unit Effects and As-Built, As-Operated Status	3
2.1.3	Licensee Participation and Peer Review	4
2.1.3.1	Licensee Participation	4
2.1.3.2	Peer Review	4
2.2	Pre-Initiator Human Action	4
2.2.1	Types of Pre-Initiator Human Actions Considered	5
2.2.2	Process for Identification and Selection of Pre-Initiators Human Actions	6
2.2.3	Screening Process for Pre-Initiator Human Actions	6
2.2.4	Quantification Process for Pre-Initiator Human Actions	7
2.3	Post-Initiator Human Actions	8
2.3.1	Types of Post-Initiator Human Actions Considered	8
2.3.2	Process for Identification and Selection of Post-Initiator Human Actions	9
2.3.3	Screening Process for Post-Initiator Human Actions	10
2.3.4	Quantification Process for Post-Initiator Human Actions	10
2.3.4.1	THERP Analyses	10
2.3.4.2	Dependency Analysis	12
2.3.5	Generic Issues and CPI	13
2.3.6	Flooding Analysis	14
2.4	Vulnerabilities, Insights and Enhancements	15

TABLE OF CONTENTS (continued)

2.4.1	Vulnerabilities	15
2.4.2	Insights Related to Human Performance	15
2.4.3	Human Performance Related Enhancements	15
3.	CONTRACTOR OBSERVATIONS AND CONCLUSIONS	17
4.	PLANT DATA	19
5.	REFERENCES	21
APPENDIX A REVIEW OF REVISED WCGS HRA ANALYSIS		A-1
A.1	Introduction	A-1
A.2	Analysis of Pre-Initiator Human Analysis	A-1
A.3	Analysis of Post-Initiator Human Analysis	A-1
A.4	Summary of Results of Requantification	A-3
A.5	Observations	A-4

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 Wolf Creek Nuclear Operating Corporation's (WCNOC) Individual Plant Examination (IPE) submittal for the Wolf Creek Generating Station (WCGS) 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

WCGS is a single-unit Westinghouse four-loop pressurized water reactor (PWR) plant rated at 1135 megawatts electric. Commercial operation started on September 3, 1985. WCGS and Callaway are sister plants designed and constructed under the Standardized Nuclear Unit Power Plant System (SNUPPS) concept. No information unique to the HRA tasks concerning the plant characteristics was presented in the submittal.

E.2 Licensee IPE Process

The WCGS IPE is comprised of a Level 1 and Level 2 PRA with internal flooding analysis. The HRA process addressed both pre-initiator and post-initiator actions. The analysis of pre-initiator events involved only restoration errors; errors in miscalibration were excluded. Post-initiator actions included both response-type and recovery-type actions. WCGS used a version of Technique for Human Error Rate Prediction (THERP) method to quantify human error; the use of this version has been found to lead to inconsistent results in other PRAs because of inherent limitations in the method. Plant-specific performance shaping factors and dependencies were considered. One human error was identified as a significant contributor in accident sequences leading to core damage, and procedure enhancements were identified and credited in the IPE HRA for events involving complete loss of CCW or SW systems. Other operator-related enhancements are under consideration.

E.3 Human Reliability Analysis

The method used for modeling both pre- and post-initiator human actions was a simplified modification of the Technique for Human Error Rate Prediction (THERP) that has been used in some other plant IPEs. In reviews of the HRA tasks of these other IPEs, this method has been identified as resulting in a lack of treatment of diagnostic operator actions, modeling only a limited number of performance-shaping factors, and using inappropriate recovery modeling. These limitations generally apply to the WCGS IPE.

The licensee, in their transmittal of their responses to the NRC's request for additional information, has undertaken to revise the HRA portion of the IPE and to report to NRC any significant changes in the accident sequence models by April 30, 1996. This review and its observations are based on the analyses presented in the existing submittal.

Pre-Initiator Human Actions

Typically, PRAs address potential errors in two types of pre-initiator human actions: 1) restoration of equipment after maintenance or test, and 2) calibration of instruments.

The licensee did include consideration of the failures of test and maintenance personnel to return valves, pumps and other system components to their normal position following test and maintenance activities. The identification of restoration actions was based on several sources of information, including system operating procedures, surveillance test procedures and typical maintenance work requests. Discussions were held with operators to ensure that the actions were modeled as performed in practice. This extent of identification is considered a strength in the WCGS IPE.

The licensee did not include miscalibration errors in the scope of the analysis, based on their seldom being identified as important in other PRAs. However, by excluding them, there is no possibility of plant-specific vulnerabilities in this area being identified. This omission of miscalibration errors is considered a limitation of the WCGS IPE.

The analysis of pre-initiator human actions involved a qualitative screening process based on such factors as whether errors would be revealed by functional system tests or by indications in the control room. No comparison with operating experience was presented to justify these screening criteria, nor were details of the application of the criteria provided for individual items of equipment to support the analysis.

Following the screening, only two pre-initiator human actions were modeled in detail. These involved failures of restoration of manual valves after testing. Neither was identified as a significant contributor to the frequency of core damage based on the THERP method. However, it is noted that unsupported assumptions concerning the likelihood of errors of commission were incorporated in these calculations; the effect of these assumptions is to reduce somewhat the failure probabilities of these events.

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

Post-Initiator Human Actions

Post-initiator human actions are divided in many PRAs into two categories: response actions taken following procedural directions, and recovery actions to recover failed functions or systems that may not be documented in plant procedures. Almost all post-initiator human actions modeled in the WCGS IPE appear to be response actions.

A total of 46 post-initiator human actions were identified and modeled using a modified version of the THERP HRA method.

A small number of recovery actions were included; one set of procedural enhancements were identified and credited for events involving complete loss of CCW or SW systems to maintain lube-oil cooling. Several other potential recovery action associated with:

- loss of CCW and SW events (to trip SI and charging pumps);
- loss of room cooling;
- loss of main and auxiliary feedwater; and
- internal flooding events

were identified and described as "under consideration."

In addition, a limited number of post-core-damage operator actions were evaluated qualitatively by the licensee as part of the back-end analysis; this evaluation was to identify any actions that would have negative consequences. One such action was identified: restarting the reactor-coolant pumps (RCPs) as directed by the procedures; this could induce a steam-generator tube rupture. No post-core-damage actions were modeled in the HRA task.

Process for Identification and Selection of Post-Initiator Human Actions. Post-initiator human actions were identified following completion of the delineation of final event trees. The actions were based on reviews of the plant procedures and talk-throughs of the actions with plant personnel, including senior reactor operators, trainers, and system analysts. The HRA analyst performed a detailed review of current plant procedures including emergency procedures, normal and abnormal operating procedures, and alarm procedures.

The types of errors considered included errors of commission, omission, diagnosis and detection, recovery, and failure to use procedure.

It is our observation that the process used to identify and select post-initiator human actions provides a reasonable assurance that important human actions have not been overlooked.

Screening Process for Post-Initiator Human Actions. No quantitative screening process for post-initiator human actions is described in the submittal. It may be inferred from the submittal that a sort of qualitative screening was performed; the submittal states that in subtask analyses "most steps which are follow through from or to some operator action and which do not involve some physical operator activity were screened out". Specific details or criteria for eliminating these actions are not discussed. It is assumed that such activities refer to generally checking system parameters while performing other tasks. This would in practice correspond with the practice in other typical HRA studies. More focused types of checking while performing specific actions are included, however. Therefore we believe it is very unlikely that important post-initiator human actions have been eliminated inappropriately by the screening process.

Quantification Process for Post-Initiator Human Actions. Modified THERP analyses were performed for most post-initiator human actions that involved tasks inside and outside the control room. In a few cases, human actions were not modeled in detail but were assigned a general judgmental human error probability.

The WCGS submittal refers to the quantification as being performed using the THERP method. However, in the sample calculations provided in response to the request for additional information, the method used was a modification of the THERP method that has been applied in a number of other IPEs, principally those that were performed using Westinghouse as a subcontractor. This method has been reviewed in the evaluations of these IPEs and found to have certain general methodological limitations. The limitations as they relate to the WCGS HRA analysis are summarized below.

The most important limitation is the lack of substantive modeling of diagnosis in the analyses. In the WCGS analyses, failure in the diagnosis process is modeled generally of failing to observe one or more indicators or alarms and omitting a step in a procedure. In this context, "diagnosis" refers to more than simply identifying the class of initiating event. It includes the actions to perceive, discriminate, and interpret an event, and the operators' decision making in responding to the event. Other HRA studies and the analyses of operational events indicate that errors in diagnosis continue to be an important factor in power-plant safety. The effect of this omission is to exclude any consideration (qualitative or quantitative) of errors in the operators' decision-making processes; this includes any consideration of the timescales in which decisions must be made.

A second limitation is the way the plant analyses have included only very simplistic evaluations of the actual plant design and operating characteristics, such as the design of the control room,

the training program, and operating experience. In consequence, the analyses only weakly reflect the plant as designed, built, and operated.

A third limitation is the selective use of a small number of human-failure modes in the analyses. Each analysis reduces human actions to only the step-by-step sequence of observing the annunciator, reading the procedure steps, and turning the switch. As well as missing any aspects of diagnosis, other THERP failure modes omitted were errors in communication, failure to use procedures, and errors incorporated in procedures. However, this is a typical limitation in other IPEs.

A final limitation is the use of inappropriate checking models (where errors by one person are recovered by another person checking the first). In several instances in the WCGS analyses, the HRA models used a checking model that is specifically described in the THERP documentation as inappropriate for analyses of post-accident human actions. This model, called the "special one-of-a-kind checking" model is identified as only to be used in routine activities like checking calibration. However, in the analyses reviewed, this model is applied to actions in the post-accident stage. The use of this checking model can have the effect of overestimating the potential for recovering from errors in the post-initiator phase, particularly because it does not include any analysis of interpersonal dependencies and only incorporates the effects of the time available for action in a very unstructured way.

It is our opinion that the calculation of failure probabilities of post-initiator human actions using this version of the THERP HRA method leads generally to inconsistent results because of the omission of failure modes associated with diagnosis, use of limited error modes and performance-shaping factors, and the use of an inappropriate recovery factor (the use of the "special" checking). An example of the inconsistencies that can result from the use of this method is the fact that the calculated likelihood of the operators failing to push the reactor scram button in an ATWS event (event RT: $1.36\text{E-}02$) is approximately an order of magnitude higher than the operators implementing feed-and-bleed operations in the event of a complete loss of secondary cooling (events OFB & OFC: $1.76\text{E-}03$). This is not considered logical given the fact that ATWS events are readily recognizable and the action is simple and taken without reference to procedures; feed-and-bleed operations are more complex, can involve several procedures, and operators can be reluctant to implement the action since they result in a bypass of one radiation barrier and result in a contaminated containment.

A limited dependency analysis was performed that examined the sensitivity of the WCGS core-damage frequency to the inclusion of dependent multiple human actions in the most significant 5000 cut sets. By removing assumptions of independence for multiple human actions in these cut sets, the core-damage frequency increased by approximately 18%. However, the final core-damage frequency and its dominant contributors identified in the submittal do not include the

effects of the dependency analysis. The limited insights provided by this sensitivity analysis (including the limited number of cut sets involving multiple human actions within the top 5000 cut sets) are considered a limitation of the IPE.

Important Operator Actions

Only one human action modeled in the HRA task was identified as a significant contributor to the WCGS core-damage frequency: OPA-RCPSEL, operators fail to provide RCP seal cooling in a timely manner, which contributes approximately 8.4% of the WCGS core-damage frequency.

In addition, the analysis of internal floods identified operator recovery actions in the event of flooding of room 3101 in the control building basement. In particular, operator actions are required to transfer the normal service water to the emergency service water operation. The core-damage frequency for the sequence involving this event is estimated to be $2.2\text{E-}06/\text{yr}$.

E.4 Generic Issues and CPI

In the evaluation of issues associated with decay heat removal, the submittal discusses the post-initiator human actions related to the decay-heat removal functions. The greatest contributions to the core-damage frequency from operator actions associated with decay heat removal are the failures to switch to high- or low-pressure recirculation; the combinations of sequences involving these failures provide a total contribution approximately $1.0\text{E-}06$ per year to the WCGS core-damage frequency.

Apart from the actions related to internal flooding described above, no other human actions were associated with any other generic issues or containment improvements.

E.5 Vulnerabilities and Plant Improvements

Vulnerabilities

The licensee identified the NUMARC 91-04 Closure Guidelines as their basis for evaluating the WCGS results for vulnerabilities. The licensee concluded that there are no plant vulnerabilities, and therefore there are no human actions associated with vulnerabilities.

Plant Improvements

The licensee identified two sets of changes that have been already incorporated in the WCGS procedures as a result of the IPE analysis; these are actions in the event of complete loss of CCW

and SW systems. The first set of actions are to supply alternate cooling water sources for lube-oil cooling for the charging and safety-injection pumps, and the second set is to trip the ECCS pumps on loss of CCW or SW. Credit for the second set of actions was modeled in the PRA since the action was already included in operator training. Credit for using alternate lube-oil cooling was not credited but is described as likely to reduce the core-damage frequency by about 7.3%.

The licensee identified six specific plant improvements that are identified as "under consideration." Four of the six would involve operator activities:

- 1) Provide a switch to bypass feedwater isolation to restore main feedwater. The current design requires operators to install jumpers to restore main feedwater manually on loss of AFW following a reactor trip. Since there is a relatively short period for the restoration, the licensee is to evaluate the installation of a switch on the main control panel. (In fact, this capability was mistakenly incorporated in the IPE because of a misunderstanding of the design freeze date, as discussed in Section 2.7.3 of the front-end Technical Evaluation Report for WCGS. The licensee estimated that its premature inclusion decreased the core-damage frequency by approximately 16%, from $5.0E-5$ to $4.2E-05$.)
- 2) Provide procedural guidance for loss of room cooling. The licensee is to consider developing procedures to supply auxiliary room cooling for selected key components on loss of room cooling.
- 3) Provide additional emergency procedures associated with total loss of CCW and SW. Currently procedures do not address comprehensively the complete loss of CCW and SW systems (see discussion above). The licensee is participating in Westinghouse Owners' Group discussions to evaluate the need for new procedures for these events.
- 4) Provide additional procedural guidance for internal flooding events. The licensee is to initiate additional evaluations of internal flooding events to identify any procedural modifications.

The licensee does not provide an estimate of the impact of the last three of these potential changes.

In addition, the licensee states that "the WCNO Training Department has integrated part of the event tree analysis information into the Operator Training Program." No particulars of what information has been integrated or any consequent changes in the training program are provided. The licensee concludes the submittal with the general intention to increase the integration of the

PRA's results into its day-to-day activities of the plant and its personnel, though again no specifics are described.

E.6 Observations

It is our general observation 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 may be 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 the factors influencing human actions to assure a realistic understanding of human performance in the plant.

In particular, the quantification method used to model human post-initiator human actions contains limitations that have been identified in this and other IPEs that can lead to inconsistent results.

A second significant limitation is the omission of any analysis of miscalibration errors from the scope of the pre-initiator human actions.

A third limitation is a lack of incorporation of human dependency modeling in the accident cut sets. While a limited dependency analysis was performed, it was only a sensitivity analysis of the top 5000 cut sets whose results are not incorporated in the IPE final results.

Other general observations include the following:

- (1) The utility actively participated in the HRA task, involving personnel from the plant's operations, training and maintenance departments.
- (2) The processes used to identify human actions to be modeled by the HRA task were reasonable and appropriate, though subject to the limitation of the exclusion of miscalibration errors.
- (3) Only one human action modeled in the HRA task was identified as a significant contributor to the frequency of core damage at WCGS; this is event OPA-RCPSEL, operators fail to provide RCP seal cooling in a timely manner, which contributes approximately 8.4% of the WCGS core-damage frequency.
- (4) Human actions were identified as important in the modeling of internal floods; these operator actions are required to transfer the normal service water to the

emergency service water operation, which requires ex-control-room actions. The probability of failure for this action is estimated to be 0.15, and is dominated by failure to access the necessary equipment areas (0.1). The core-damage frequency for the sequence involving this event is estimated to be $2.2\text{E-}06/\text{yr}$.

- (5) The licensee identified four specific plant improvements that would involve operator activities; these improvements are identified as "under consideration", although one was prematurely incorporated in the IPE (provision of the feedwater isolation bypass switch). One additional action, to provide alternate cooling to the charging and safety injection pumps, has been incorporated in the WCGS procedures. It was not credited in the IPE, but was estimated to reduce the core-damage frequency by approximately 7.3%.

It is recognized that the licensee has decided to re-perform the HRA task of the IPE with the intention of eliminating many of the limitations in the analysis. It can be expected that the changes in the HRA modeling will significantly change the results and findings of both the front-end and back-end portions of the IPE because of changes in the sequences that will dominate the risk of core damage at WCGS.

1. INTRODUCTION

This Technical Evaluation Report (TER) is a summary of the review of the human reliability analysis (HRA) presented as part of the Wolf Creek Generating Station (WCGS) Individual Plant Examination (IPE) submittal 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. This section of the TER highlights findings from the technical review.

1.1 Review Process

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

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

Findings and conclusions are limited to those that could be supported by the document-only review; no visit to the site was conducted. It was not the intent of the review to reproduce results or verify in detail the licensee's HRA quantification process. The review addressed the reasonableness of the overall approach with regard to its ability to permit the licensee to meet the goals of Generic Letter 88-20.

1.2 Plant Characterization

WCGS is a single-unit Westinghouse four-loop pressurized water reactor (PWR) plant rated at 1135 megawatts electric. Commercial operation started on September 3, 1985. WCGS and Callaway are sister plants designed and constructed under the Standardized Nuclear Unit Power Plant System (SNUPPS) concept. The unit has a plant-specific simulator, which was used in the development of the HRA.

2. TECHNICAL REVIEW

2.1 Licensee IPE Process

The WCGS IPE is comprised of a Level 1 and Level 2 PRA with internal flooding analysis. The HRA process addressed both pre-initiator and post-initiator actions. The analysis of pre-initiator events involved only restoration errors; errors in miscalibration were excluded. Post-initiator actions included both response-type and recovery-type actions. WCGS used a modified version of the Technique for Human Error Rate Prediction (THERP) method to quantify human error events; this method has been used in some other IPEs. Some plant-specific performance shaping factors and dependencies were considered. One human error was identified as a significant contributor in accident sequences leading to core damage, and procedure enhancements were identified and credited in the IPE HRA for events involving complete loss of CCW or SW systems.

Licensee staff with knowledge of plant design, operations and maintenance had significant involvement in the HRA process. Procedures reviews, interviews with operations staff, and plant walkdowns helped assure that the IPE represented the as-built, as-operated plant. Independent reviews of the HRA were performed by an internal Nuclear Safety Engineering Group and the Union Electric IPE external review team.

2.1.1 Completeness and Methodology.

With the exception of the exclusion of miscalibration errors from the scope of pre-initiator human actions, the analysis covered all types of human actions usually addressed in PRAs. The exclusion of miscalibration errors is, however, an important limitation in the analysis--especially the potential for common-mode miscalibration errors for important reactor parameters such as RCS pressure and pressurizer level. The licensee provides several reasons for excluding these errors, including the facts that no such events were identified in the WCGS data and that such errors have rarely been found important in other PRAs. However, the period of operational data reviewed is relatively short (late 1985 to 1990), and does not demonstrate that such failures cannot occur. The omission of any search for miscalibration opportunities at Wolf Creek means simply that any potential plant-specific vulnerabilities in this area will not be identified, and represents a limitation of the IPE.

The methodology used for the HRA study in the WCGS study was a modification of THERP that has been used in other IPEs. Reviews of the HRA portion of these other IPEs have identified this version of THERP to result in significant limitations in the IPEs.

This method is generally based on the THERP method reported in NUREG/CR-1278 (Ref. 1), but with important differences in the data and the modeling process. This method is considered deficient for the following reasons, which are discussed in more detail in section 2.3.4.1 of the report:

- the lack of modeling of diagnosis in the analyses of post-initiator human actions;
- the inclusion of very limited plant-specific evaluations of the actual plant's design and operating characteristics, such as the design of the control room, the training program, and operating experience;
- the use of a very limited set of human-failure modes in the analyses (such as only failures from omitting a step in a procedure or selecting a wrong switch); and
- the use of inappropriate checking models, where errors by one person are recovered by another person checking the first.

In the cover letter providing the responses to the NRC's requests for additional information, the licensee stated that they are planning to revise the HRA portion of the IPE "to improve the utilization of performance shaping factors, diagnostic errors, incorporation of plant-specific practices and experiences, and dependencies of operator actions." These areas for revision are those of concern identified in the methodology review. The licensee intends to complete the revision by April 30, 1996; the consequential changes to core-damage sequences will be notified to NRC.

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

The NRC review of the submittal attempts to determine whether the utility personnel were involved in the development and application of PRA techniques to their facility, and that the associated walkdowns and documentation reviews constituted a viable process for confirming that the IPE represents the as-built and as-operated plant.

Wolf Creek is a single unit station. The WCNOG established a permanently assigned staff to be involved with all aspects of the PRA. This team, with the assistance of other WCGS personnel and a contractor, assembled and utilized current plant documentation, performed multiple walkdowns, and conducted operator talk-throughs during the information assembly process.

Three walkdowns, supported by check lists, were conducted by the PRA team; (1) System Walkdowns - support of the system fault tree analysis, (2) Containment Walkdowns - all elevations and compartments including appropriate portions of the Auxiliary Building containing potential bypass methods, and (3) Internal Flooding Walkdowns - general location and orientation of critical equipment to obtain relationship for specific hazards identification during analysis.

The analyst performing the HRA conducted talk-throughs of procedural actions with the plant operators. Specific objectives for these discussions include increasing the analyst's familiarity with required tasks and time constraints involved with performance of tasks and ensuring that the modeling was consistent with the procedures as performed by plant personnel.

The process as applied appears capable of assuring the analyses adequately reflect the as-built, as-operated plant to the degree that the models incorporate factors associated with the plant's design and operation.

2.1.3 Licensee Participation and Peer Review.

2.1.3.1 Licensee Participation. The description of the IPE program's organization provided by the licensee does not specifically describe the HRA tasks. It is inferred that the work comprising the HRA task was performed primarily by contractor personnel with active participation of licensee staff; it is stated that training was provided to licensee staff in the methodologies used in the PRA. Plant personnel involved in the study included staff from operations, training, plant engineering, licensing and safety analysis groups.

It is stated that maintenance, training, and operations personnel participated in the identification of human actions modeled in the HRA analyses.

2.1.3.2 Peer Review. Two levels of independent review were performed on the WCGS IPE. The first was an in-house review by the licensee's Nuclear Safety Engineering group. The members of this group are described as being comprised of nuclear, mechanical, and electrical engineers; no operations personnel nor experts in HRA are identified as being involved in this in-house review. The second independent review was performed by the Union Electric IPE team. This group was responsible for performing the IPE for Callaway, a sister plant of Wolf Creek.

In addition to these independent reviews, Westinghouse and WCNOC personnel also reviewed the work performed during the IPE process.

The licensee presents three examples of comments received during these peer reviews; none are directly associated with the HRA task.

2.2 **Pre-Initiator Human Actions**

Errors in performance of pre-initiator human 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 of the HRA portion of the IPE examines the licensee's HRA process to determine what consideration was given to pre-initiator human events, how potential events were identified, the effectiveness of quantitative and qualitative screening processes employed, and the processes for accounting for plant-specific performance shaping factors, recovery factors, and dependencies among multiple actions.

2.2.1 Types of Pre-Initiator Human Actions Considered.

Typically, PRAs address potential errors in two types of pre-initiator human actions: 1) restoration of equipment after maintenance or test, and 2) calibration of instruments.

The licensee did include consideration of the failures of test and maintenance personnel to return valves, pumps and other system components to their normal position following test and maintenance activities.

The licensee did not include miscalibration errors. Four reasons are given for miscalibration errors not being included:

- 1) historical data for WCGS do not show miscalibration failures;
- 2) such errors would be as likely to produce an early actuation as a delayed or prevented actuation;
- 3) there are normally multiple input signals or actuation devices; and
- 4) miscalibration errors have seldom been shown to be important in past probabilistic risk assessments.

This omission of miscalibration errors is considered a limitation of the WCGS IPE. While it is generally true that such errors are rarely identified as significant in PRAs, this is partly because several studies have similarly not excluded them from the scope of the analysis. In contrast, other PRAs have identified such errors as potentially important.

In addition, errors in instrumentation (including miscalibration errors) have played significant roles in operational events, such as those described in recent NRC reports (Ref. 2). In PWRs like Wolf Creek, certain parameters such as pressurizer water level and pressure are important in diagnosing the state of the plant; erroneous calibration of instrumentation associated with these parameters can lead to important post-initiator operator and other system failures. By excluding miscalibration errors (particularly any common-cause errors) from the scope of the analysis, any potential plant-specific vulnerabilities cannot be found regardless of the significance (or not) of such errors in other PRAs.

In addition, the absence of plant experience of miscalibration events is one reason cited above for their exclusion. However it must be noted that the period of experience for the use of plant-specific information is only from September 1985 (the start of commercial operation) to the end of 1990.

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

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

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 operations, testing, and maintenance, as defined in the WCGS system operating procedures, surveillance test, and maintenance procedures, technical specifications, and typical maintenance work requests. Those components whose changes of state during operations, 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.

2.2.3 Screening Process for Pre-Initiator Human Actions.

No numerical screening process was applied for the pre-initiator human actions. A non-numerical screening process was used by the licensee to eliminate many potential pre-accident human actions from the detailed HRA quantification process. The screening rules for the pre-accident human actions were to exclude from further consideration a component (pump or valve) if any of the following criteria were met.

- valve or other component mis-positioning is detectable by status lights or alarms at the main control panel;
- proper valve positioning can be detected using specified pump flow tests; and
- the valve is automatically realigned by an ESFAS signal.

No list is provided for the pre-accident human actions screened out using these criteria. A total of two sets of pre-accident human actions remained following the screening process. These sets are comprised of valves not restored or realigned following testing of the valves associated with

the turbine-driven auxiliary feedwater pump (OPA-ALHVS), and the main steam system (OPA-ABVLS).

2.2.4 Quantification Process for Pre-Initiator Human Actions.

The two pre-accident human actions that were not screened out using the criteria in Section 2.2.3 were quantified using the Westinghouse interpretation of the Technique for Human Error Rate Prediction (THERP) (Ref. 1). These calculations incorporate assumptions about the operating experience and "proper labeling" to lead to a reduction in the likelihoods of errors of commission by a factor of 10; however, no supporting evidence for these assumptions is supplied and the reduction is considered inappropriate in the absence of such evidence.

The values calculated for each of the pre-accident human action error probabilities is given in Table 1.

Examples of the calculation process for quantifying these pre-initiator human actions indicates that the assessment of performance-shaping factors was limited to selection of a wrong control, the existence, length, type and use of procedures, and the recovery through routine checking actions.

Table 1. Summary of pre-accident human actions

Event Name	Human Action Description	Failure Probability
OPA-ALHVS	Reopen valve ALHV0006 following TD AFW pump in-service test (also applies to valves ALHV0008, 0010, and 0012)	8.3E-04
OPA-ABVLS	Reopen valve ABV0018 following in-service valve test of SG PORV (also applies to valves ABV0007, 0029, and 0040)	3.7E-04*

*In the response to NRC's request for additional information (RAI), the licensee identified event OPA-ABVLS modeled in the original submittal did not include failures resulting from errors of commission. Including such errors increases the probability of event OPA-ABVLS to 4.3E-04. The licensee states that this change does not have a significant impact on the IPE results.

Generally these failure probabilities lie within a range of 10 or less of similar failure probabilities calculated in those submittals that have modeled pre-initiator human actions associated with failures to restore valves following test or maintenance. For example, using the generic ASEP method, without credit for any plant-specific features (labeling, periodic checks, etc.), would indicate a failure probability of 3.0E-03. Therefore we believe that the failure probabilities presented in Table 1 are reasonable.

Overall the information from the licensee regarding the assessment of pre-initiator human actions indicates that the assessment was relatively narrow in scope and limited in depth. Calibration

errors were discounted without a thorough justification being presented. The scope of the assessment of restoration errors appears to be limited to valves, and the detailed analysis limited to two sets of valves. The THERP calculations appear to have been executed properly, though with unjustified assumptions about reductions in the failure probabilities of errors of commission. While these limitations may or may not have a significant impact on the gross quantitative results of the IPE or the basic conclusions drawn from the study, they do limit the potential for the licensee to gain a full appreciation of the ways in which human performance can influence overall risk and to identify potential risk-reduction measures. In some PRAs more rigorous assessments of pre-initiator human actions have determined that they are significant contributors to risk, and some enhancements have been made that have contributed to an overall estimated reduction of risk based on the assessment of pre-initiator human actions.

2.3 Post-Initiator Human Actions

Human error in responding to an accident initiator (for example by not recognizing and diagnosing the situation properly, or failure to perform required activities as directed by procedures) can have a significant effect on plant risk, and in some cases have been shown to be dominant contributors to core-damage frequency. These errors are referred to as post-initiator human errors. 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, including issues such as the means for evaluating timing, dependency among human actions, and other plant-specific performance shaping factors.

2.3.1 Types of Post-Initiator Human Actions Considered.

There are two important types of post-initiator actions considered in most PRAs: response actions, which include those human actions performed in response to the first level directives of the emergency operating procedures or instructions (EOPs, or EOIs); and, recovery 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.

Section 3.3.3 states that human actions considered recovery from each initiating event; only procedure-based actions were considered. These actions appear to be more appropriately termed "response" actions. Elsewhere it is stated that "recovery" (in the sense of actions taken to restore failed systems or functions and that are not described in procedures) was also included, and one set of procedural enhancements were identified and credited in the IPE HRA for events involving complete loss of CCW or SW systems, to maintain lube-oil cooling. Several other potential recovery action associated with:

- loss of CCW and SW events (to trip SI and charging pumps);
- loss of room cooling;

- loss of main and auxiliary feedwater; and
- internal flooding events

were identified and described as "under consideration."

In addition, a limited number of post-core-damage operator actions were evaluated qualitatively by the licensee as part of the back-end analysis; this evaluation was to identify any actions that would have negative consequences. One such action was identified: restarting the reactor-coolant pumps (RCPs) as directed by the procedures; this could induce a steam-generator tube rupture. No post-core-damage actions were modeled in the HRA task.

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.

Post-initiator human actions were identified following completion of the delineation of final event trees. The actions were based on reviews of the plant procedures and talk-throughs of the actions with plant personnel, including senior reactor operators, trainers, and system analysts. The HRA analyst performed a detailed review of current plant procedures including:

- Emergency Procedures (EMG's);
- Normal and Abnormal Operating Procedures (OFN's); and
- Alarm Procedures (ALP's).

The talk-throughs between the HRA analyst and plant staff on procedural actions resulted in some actions being dropped and other added.

The types of errors considered included errors of commission, omission, diagnosis and detection, recovery, and failure to use procedure.

It is observation that the process used to identify and select post-initiator human actions provides a reasonable assurance that important human actions have not been overlooked.

2.3.3 Screening Process for Post-Initiator Human Actions.

No quantitative screening process for post-initiator human actions is described in the submittal. It may be inferred from the submittal that a sort of qualitative screening was performed, which states that in subtask analyses "most steps which are follow through from or to some operator action and which do not involve some physical operator activity were screened out". Specific details or criteria for eliminating these actions are not discussed. It is assumed that such activities refer to generally checking system parameters while performing other tasks. This would in practice correspond with the practice in other typical HRA studies. More focused checking while performing specific actions are included, however. Therefore we believe that it is very unlikely that important post-initiator human actions have been eliminated inappropriately by the screening process.

2.3.4 Quantification Process for Post-Initiator Human Actions.

Modified THERP analyses were performed for most post-initiator human actions that involved tasks inside and outside the control room. In a few cases, human actions were not modeled in detail but were assigned a general judgmental human error probability.

2.3.4.1 Modified THERP Analyses. The WCGS submittal refers to the quantification as being performed using the THERP method described in NUREG/CR-1278 (Ref. 1). However, in the sample calculations provided in response to the request for additional information, the method used was a modification of the THERP method that has been applied in a number of other IPEs, principally those that were performed using Westinghouse as a subcontractor. This method has been reviewed in the evaluations of these IPEs and found to have certain general methodological limitations. The limitations as they relate to the WCGS HRA analysis are summarized below.

The most important limitation is the lack of substantive modeling of diagnosis in the analyses. In the WCGS analyses, failure in the diagnosis process is modeled generally of failing to observe one or more indicators or alarms and omitting a step in a procedure.

Problems in diagnosis were shown to be an important factor in several operational events analyzed recently by NRC, including those events described in Volume 8 of NUREG-1275 (Ref. 2). In this context, "diagnosis" refers to more than simply identifying the class of initiating event. It includes the actions to perceive, discriminate, and interpret an event, and the operators' decision making in responding to the event. Other HRA studies, as well as the analyses of operational events such as those discussed in NUREG-1275, indicate that errors in diagnosis continue to be an important factor in power-plant safety.

The effect of this omission is to exclude any consideration (qualitative or quantitative) of errors in the operators' decision-making processes; this includes any consideration of the timescales in which decisions must be made, for example.

A second limitation is the way the plant analyses have included only very simplistic evaluations of the actual plant design and operating characteristics, such as the design of the control room, the training program, and operating experience. The submittal does not include any discussion of the standards used to judge these factors (for example, comparisons with other plants, the findings of detailed control-room reviews or procedure reviews, or evaluations of operating and maintenance programs in NRC's SALP inspections). In consequence, the analyses only weakly reflect the plant as designed, built, and operated.

A third limitation is the selective use of a small number of human-failure modes in the analyses. Each analysis reduces human actions to only the step-by-step sequence of observing the annunciator, reading the procedure steps, and turning the switch. As well as missing any aspects of diagnosis, other THERP failure modes omitted were errors in communication, failure to use procedures, and errors incorporated in procedures. However, this is a typical limitation in other IPEs.

A final limitation is the use of inappropriate checking models (where errors by one person are recovered by another person checking the first). In several instances in the WCGS analyses, the HRA models used a checking model that is specifically described in the THERP documentation as inappropriate for analyses of post-accident human actions. This model, called the "special one-of-a-kind checking" model is identified as only to be used in routine activities like checking calibration. However, in the analyses reviewed, this model is applied to actions in the post-accident stage. The use of this checking model can have the effect of overestimating the potential for recovering from errors in the post-initiator phase, particularly because it does not include any analysis of interpersonal dependencies and only incorporates the effects of the time available for action in a very unstructured way.

The review of example events indicates that these deficiencies in the version of THERP are present in the WCGS analyses. Consider, for example, the case of event OPA-RCPSEL, operator provides RCP seal cooling flow in a timely manner; this human action event is identified as the highest contributing human failure event to the WCGS core-damage frequency. The actions involved are: following recognition of the failure of operating CCW train A and successful switchover to CCW train B, to align the RCP seal service loop to CCW train B. This is modeled as successful completion of two operator actions:

- transfer service loop to train B; and
- isolate service loop from train A.

Both actions are modeled using two similar error modes: select wrong control, and omit step in procedure.

The quantification assumes a high stress because of the short time available for action (6 minutes); that the error of commission, of miss-selecting the control, is a factor of 10 lower than corresponding errors of omission; and that the omission involves omitting a step from a short procedure (<10 steps) with checkoff.

There is no consideration of diagnostic requirements, including observing any alarms or interpreting them. The transfer of the CCW trains that precede the operator action are modeled only as an equipment operation; no related human action is listed for that transfer in Sequence 13, for example. Such an omission is considered an important limitation in this event, and, by extension, in the WCGS HRA analysis as a whole.

Other limitations discussed above are present in the modeling of other events. For example, in the evaluation of event OPA-LC1, operator initiates low-head recirculation, a recovery step includes correcting earlier errors by "special short-term, one-of-a-kind checking with alerting factors." As discussed earlier, this factor is specifically excluded from the modeling of post-initiator human actions according to NUREG/CR-1278.

It is our opinion that the calculation of failure probabilities of post-initiator human actions using this version of the THERP HRA method leads generally to inconsistent results because of the omission of failure modes associated with diagnosis, use of limited error modes and performance-shaping factors, and the use of an inappropriate recovery factor (the use of the "special" checking). An example of the inconsistencies that can result from the use of this method is the fact that the calculated likelihood of the operators failing to push the reactor scram button in an ATWS event (event RT, $1.36\text{E-}02$) is approximately an order of magnitude higher than the operators implementing feed-and-bleed operations in the event of a complete loss of secondary cooling (events OFB & OFC, $1.76\text{E-}03$). This is not considered logical given the fact that ATWS events are readily recognizable and the actions are simple and taken without reference to procedures; feed-and-bleed operations are more complex, can involve several procedures, and operators can be reluctant to implement the actions since they result in a bypass of one radiation barrier and result in a contaminated containment.

2.3.4.2 Dependency Analysis. A limited but unspecified number of human actions were identified as occurring in accident sequences that already included one or more post-initiator human errors. The modeling of these events was performed explicitly using a dependency analysis method. The submittal recognizes that the dependency analysis was only partially implemented at the time of performing the submittal.

These events were quantified with the aid of a decision tree that guided the analyst to assessing whether the degree of dependence was considered high, moderate, or low. According to the degree of dependence, a failure probability conditional on the previous error event was calculated. Broadly these probabilities corresponded to the values cited as low, moderate, and high dependence conditional probabilities in Table 20-17 of NUREG/CR-1278.

The decision tree considered five factors in assessing the degree of dependence. These were:

- 1) the level of stress in the prior event;
- 2) the time window for the second event (i.e., the time available for the action to be performed before system failures occur);
- 3) the amount of slack time for the second event (i.e., the difference between the time window and the time required for responding);
- 4) the complexity involved in the second event (i.e., the number of steps required to perform the task); and
- 5) the simplicity of procedural guidance for the second event (i.e., more than one procedure required or the steps are ambiguous or confusing).

No explanation is provided by the licensee as to why these particular factors are important influences in one human action being dependent on a prior human error in an accident scenario. For example, one combination of factors--a low stress level in the prior action combined with a short time window and small slack time for the second action--yields a high dependence.

The selection of factors does not appear to be based on any underlying models or understanding of coupling mechanisms between human errors, such as those discussed in Chapter 10 of NUREG/CR-1278, those incorporated in the ASEP HRA dependence model described in NUREG/CR-4772 (Ref. 3), or those discussed in other HRA literature. In the absence of an explanation for the selection of factors, an intuitive justification can be made that failure in the earlier event and its associated stress, combined with poor PSFs for the task being performed, will lead to a higher failure probability than when the task is being performed with no prior failure. It should also be noted that the factors as applied, would seem generally to lead towards conservative probabilities for most of the events analyzed.

Within the performance of the IPE, only the most significant 5000 cut sets were reviewed for potential dependencies. By using the dependency model, the core-damage frequency was increased by approximately 18% compared with using assumptions of independence. However, it is unclear how many of these most significant 5000 cut sets included human action events. Further, the assumption of independence would have the effect of potentially eliminating important cut sets from the top sequence contributors, and therefore these top 5000 cut sets will not incorporate all potentially important sequences involving human actions. This limited analysis of dependencies is considered a limitation in the WCGS IPE.

2.3.5 Generic Issues and CPI.

In the evaluation of issues associated with decay heat removal, the submittal discusses the post-initiator human actions related to the following functions:

- For a transient event with PCS available, if the AFW system is not available, the operators are directed to establish an alternative feedwater supply.
- With no feedwater flow to the steam generators, the operators are directed to initiate primary-side feed-and-bleed cooling per emergency guideline FR-H1. The probability of the operators failing to diagnose and perform the feed-and-bleed operation is assessed to be $1.8\text{E-}03$.
- During injection, when the low-level RWST alarm setpoint is reached, the operators transfer suction of the ECCS from the injection to the recirculation mode. The probability of the operators failing to transfer to high-pressure recirculation is $5.0\text{E-}04$ and to low-pressure recirculation is $9.2\text{E-}04$.
- Long-term decay heat removal with the RCS pressure above the shut-off head of the RHR pumps can be accomplished by the operators aligning the suction of the high-pressure ECCS pumps to the discharge of the low-pressure ECCS pumps. The probability of failure for this operator action is $1.5\text{E-}03$.
- Long-term decay heat removal with the RCS pressure below the shut-off head of the RHR pumps can be accomplished by the continued operation of the low-pressure recirculation system. Operator action is required to accomplish this operation. The probability of failure for this operator action is $9.2\text{E-}04$.

The greatest contributions to the core-damage frequency from operator actions associated with decay heat removal are the failures to switch to high- or low-pressure recirculation. The sequences involving these failures contribute approximately $1.0\text{E-}06$ per year.

No human actions were identified with other generic issues or containment performance improvements, except for the analysis of internal flooding discussed below.

2.3.6 Flooding Analysis.

The analysis of internal floods identifies operator recovery actions in the event of flooding of room 3101 in the control building basement. In particular, operator actions are required to transfer the normal service water to the emergency service water operation. This requires ex-control-room actions. The probability of failure for this action is estimated to be 0.15, and is dominated by failure to access the necessary equipment areas (0.1). The analysis provides no direct information as to the time within which this action must be carried out, nor the time required to access the room and perform the actions. Therefore it is not possible to form an opinion as to the appropriateness of this probability. The core-damage frequency for the sequence involving this event is estimated to be $2.2\text{E-}06/\text{yr}$.

Operator actions are not identified for any other accident sequences involving internal floods.

2.4 Vulnerabilities, Insights and Enhancements

2.4.1 Vulnerabilities.

The licensee identified the NUMARC 91-04 Closure Guidelines as their basis for evaluating the WCGS results for vulnerabilities. The licensee concluded that there are no plant vulnerabilities.

2.4.2 Insights Related to Human Performance.

In the evaluation of major contributors to core damage, only one operator action modeled in the HRA task is identified: OPA-RCPSEL, operators fail to provide RCP seal cooling in a timely manner, which contributes approximately 8.4% of the WCGS core-damage frequency. Other events involve operator activities, such as restoration of AC power within 8 hours of SBO (13.9%), and AC power not restored within 2 hours of SBO (3.8%). These actions to restore AC power are modeled, like in most other PRA, as parametric distributions of the probability of power recovery versus time and not using HRA modeling.

In addition, the licensee confirms that no core-damage accident sequences dropped below the screening criteria of the NRC's Generic Letter 88-20 because of recovery actions being credited by a factor of lower than 0.1.

2.4.3 Human Performance Related Enhancements.

The licensee has identified two sets of changes that have been already incorporated in the WCGS procedures as a result of the IPE analysis; these are actions in the event of complete loss of CCW and SW systems. The first set of actions are to supply alternate cooling water sources for lube-oil cooling for the charging and safety-injection pumps, and the second set is to trip the ECCS pumps on loss of CCW or SW. Credit for the second set of actions was modeled in the PRA since the action was already included in operator training. Credit for using alternate lube-oil cooling was not taken but was estimated as likely to reduce the core-damage frequency by about 7.3%.

The licensee identified six specific plant improvements that are identified as "under consideration." Four of the six would involve operator activities:

- 1) Provide a switch to bypass feedwater isolation to restore main feedwater. The current design requires operators to install jumpers to restore main feedwater manually on loss of AFW following a reactor trip. Since there is a relatively short period for the restoration, the licensee is to evaluate the installation of a switch on the main control panel. (In fact, this capability was mistakenly incorporated in the IPE because of a misunderstanding of the design freeze date, as discussed in Section 2.7.3 of the front-end Technical Evaluation Report for WCGS. The licensee estimated that its premature inclusion decreased the core-damage frequency by approximately 16%, from 5.0E-5 to 4.2E-05.)

- 2) Provide procedural guidance for loss of room cooling. The licensee is to consider developing procedures to supply auxiliary room cooling for selected key components on loss of room cooling.
- 3) Provide emergency procedures associated with total loss of CCW and SW. Currently procedures do not address complete loss of CCW and SW systems (see discussion above). The licensee is participating in Westinghouse Owners' Group discussions to evaluate the need for procedures for these events.
- 4) Provide additional procedural guidance for internal flooding events. The licensee is to initiate additional evaluations of internal flooding events to identify any procedural modifications.

The licensee does not provide an estimate of the impact of the last three of these potential changes.

In addition, the licensee states that "the WCNOG Training Department has integrated part of the event tree analysis information into the Operator Training Program." No particulars of what information has been integrated or any consequent changes in the training program are provided. The licensee concludes the submittal with the general intention to increase the integration of the PRA's results into its day-to-day activities of the plant and its personnel, though again no specifics are described.

3. CONTRACTOR OBSERVATIONS AND CONCLUSIONS

The intent of our document-only review of the licensee's HRA process 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 necessary/appropriate, implement reasonable human-performance related enhancements.

It is our general observation 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 may be 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 the factors influencing human actions to assure a realistic understanding of human performance in the plant.

In particular, the quantification method used to model human post-initiator human actions contains limitations that have been identified in this and other IPEs that can lead to inconsistent results.

A second significant limitation is the omission of any analysis of miscalibration errors from the scope of the pre-initiator human actions.

A third limitation is a lack of incorporation of human dependency modeling in the accident cut sets. While a limited dependency analysis was performed, it was only a sensitivity analysis of the top 5000 cut sets whose results are not incorporated in the IPE final results.

Other general observations include the following:

- 1) The utility actively participated in the HRA task, involving personnel from the plant's operations, training and maintenance departments.

- 2) The processes used to identify human actions to be modeled by the HRA task were reasonable and appropriate, though subject to the limitation of the exclusion of miscalibration errors.
- 3) Only one human action modeled in the HRA task was identified as a significant contributor to the frequency of core damage at WCGS; this is event OPA-RCPSEL, operators fail to provide RCP seal cooling in a timely manner, which contributes approximately 8.4% of the WCGS core-damage frequency.
- 4) Human actions were identified as important in the modeling of internal floods; these operator actions are required to transfer the normal service water to the emergency service water operation, which requires ex-control-room actions. The probability of failure for this action is estimated to be 0.15, and is dominated by failure to access the necessary equipment areas (0.1). The core-damage frequency for the sequence involving this event is estimated to be $2.2\text{E-}06/\text{yr}$.
- 5) The licensee identified four specific plant improvements that would involve operator activities; these improvements are identified as "under consideration", although one was prematurely incorporated in the IPE (provision of the feedwater isolation bypass switch). One additional action, to provide alternate cooling to the charging and safety injection pumps, has been incorporated in the WCGS procedures. It was not credited in the IPE, but was estimated to reduce the core-damage frequency by approximately 7.3%.

It is recognized that the licensee has decided to re-perform the HRA task of the IPE with the intention of eliminating many of the factors that have led to the recommended rejection of the analysis. It can be expected that the changes in the HRA results will significantly change the results and findings of both the front-end and back-end portions of the IPE because of changes in the sequences that will dominate the risk of core damage at WCGS.

4. PLANT DATA

4.1 Important Operator Actions

In the evaluation of major contributors to core damage, only one operator action modeled in the HRA task is identified: OPA-RCPSEL, operators fail to provide RCP seal cooling in a timely manner, which contributes approximately 8.4% of the WCGS core-damage frequency. Other events involve operator activities, such as restoration of AC power within 8 hours of SBO (13.9%), and AC power not restored within 2 hours of SBO (3.8%).

Table 1 identifies the human action events analyzed in the WCGS IPE.

Table 1

Event	Operator Action	HEP
?	Fail to manually actuate safety injection within 20 minutes	1.02E-04
ABVLS	Failure to reopen isolation valve after STS AB-201 performance	3.74E-04
ACNN	Provide alternate source to 120 VAC bus	2.60E-02
AFC	Maintain AFW flow during station blackout	1.36E-04
ALHVS	Reopen air-operated valve	8.29E-04
CSS	Switchover containment spray system	1.70E-03
DCNK01	Manually transfer NB01 components on NK01 failure	4.77E-03
EC3	Long term cooldown and depressurization, given SGTR	2.15E-04
ECCSTP	Manually trip ECCS pumps	1.00E-02
ES1	Long term cooldown and depressurization, given small LOCA	1.35E-04
ESWA	Realign ESW A to normal service water	1.10E-03
ESWAB	Place emergency service water system into operation	2.40E-04
ESWABF	Switch ESW due to flood	1.46E-01
ESWB	Realign ESW B to normal service water	1.10E-03
IEHVAC	Loss of SGK05A and SGK05B A/C Units	1.00E-01
LC1	Perform low-head recirculation	9.17E-04
LC2/LC3	Perform high pressure recirculation	4.97E-04
LTS	Long-term shutdown	4.38E-05
MCB	Manually start component on auto start failure	1.59E-03
MF1	Establish MFW flow	6.02E-04
MRT	Manually trip RDGMs	1.55E-01
MS1	Isolate ruptured SG	1.59E-03
OD1-COOL	Initial RCS cooldown, given SG rupture	5.55E-03
OD1-DP	Initial RCS Depressurization, given SG tube rupture	9.55E-03
OD2	Stabilize RCS and ruptured SG after SG overfills	2.90E-03
OFB & OFC	Initiate feed and bleed	1.76E-03
OP1	RCS cooldown and depressurization, given medium LOCA with HPSI failure	1.73E-04
OP2	RCS cooldown and depressurization, given small LOCA with HPSI failure	1.09E-04
OST	Terminate HPSI	5.78E-05
PEG1BD	Switch-over CCW Operation to Train B	9.42E-03
PEG1C	Manually start CCW pump	6.04E-03
RCD1	RCS cooldown during blackout	1.66E-03
RCD2	RCS cooldown during loss of CCW	1.32E-04
RCPSEL	Provide RCP seal injection flow	1.43E-02
RCPTRP	Manually trip RCPs	2.39E-03
RHR	Stop RHR pumps	5.01E-04
RR11	Restore RCS inventory using 1 of 1 train	5.64E-03
RR12	Restore RCS inventory using 1 of 2 trains	9.88E-04

9/05/96

Event	Operator Action	HEP
RR122	Restore RCS inventory using 2 of 2 trains	7.35E-03
RT	Manually trip reactor or insert rods	1.36E-02
RUPSG	Identify ruptured SG	6.33E-05
SBCOOL	Fail to restore auxiliary cooling to DC SWBD Rooms on loss of HVAC	1.00E-01
SGTR	Diagnose SGTR event	6.36E-06
SIAO,SIBO	No ESFAS signal, one train available, with operator action	3.90E-03
SYSIEV	Return ESW B train to normal service water	2.16E-02
WESFO	No ESFAS signal, both trains available, with operator action	3.19E-05
WS1C2	Start standby service water pump	1.48E-04

4.2 Human Performance Related Enhancements

As a consequence of performing the IPE, the licensee has identified one set of changes that have been already incorporated in the WCGS procedures as a result of the IPE analysis; these are actions in the event of complete loss of CCW and SW systems to supply alternate cooling water sources for lube-oil cooling for the charging and safety-injection pumps.

5. REFERENCES

1. Swain, A. D. and H. E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, Rev. 1, Sandia National Laboratories, Albuquerque, NM, August 1983.
2. Kauffman, J. V., et al., *Operating Experience Feedback Report - Human Performance in Operating Events*, NUREG-1275, Vol. 8, U.S. Nuclear Regulatory Commission, Washington, DC, December 1992.
3. Swain, A. D., *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*, NUREG/CR-4772, Sandia National Laboratories, Albuquerque, NM, February 1987.

APPENDIX A, REVIEW OF REVISED WCGS HRA ANALYSIS

A.1 Introduction

Following submittal of the WCGS IPE, the licensee indicated to NRC that they intended to revise significantly the human reliability analysis, as outlined in the introduction of the main body of this report. The licensee did indeed make these modifications and reported the results of these revisions to NRC as an attachment to a letter dated May 30, 1996¹. This appendix summarizes a review of these revisions.

The principal revision was to change the method used to analyze and quantify the post-initiator human action events. The original WCGS HRA modeling was performed using a modified version of THERP, as described in Section 2 of this report. 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 omission of analysis of dependencies between human actions. In addition, the licensee provided an analysis of a certain number of calibration actions; the original submittal excluded calibration actions from the scope of that analysis.

A.2 Analysis of Pre-Initiator Human Actions

One limitation of the WCGS IPE identified in Section 2 of this report was the exclusion of errors in pre-initiator calibration actions.

As part of the revisions in the HRA portion of the IPE, the licensee performed a limited analysis of calibration actions. Specifically, five calibration human action events were modeled, associated with the refueling water storage tank (RWST) level, auxiliary feedwater (AFW) pumps' suction pressure, and the diesel fuel-oil day tank level. (Other IPEs have identified miscalibration of the RWST as a potentially significant human action event.) The analysis of calibration actions was performed using the Technique for Human Error-Rate Prediction (THERP).

Other limitations in the analysis of pre-initiator human actions, such as the screening process and the reductions of calculated human error probabilities, were unchanged in the revisions.

A.3 Analysis of Post-Initiator Human Actions

The licensee has reanalyzed the post-initiator human actions using the Cause-Based Decision Tree (CBDT) Method developed by the Electric Power Research Institute (EPRI)². 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.

¹. Letter, Richard A. Muench, Wolf Creek Nuclear Operating Station, to U.S. Nuclear Regulatory Commission, Reference ET 96-0034, Docket No. 50-482, dated May 30, 1996.

². EPRI TR-100259, An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment, Electric Power Research Institute, Palo Alto, CA, June 1992.

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:

- a. availability of relevant indications (location, accuracy, reliability of indications);
- b. attention to indications (workload, monitoring requirements, relevant alarms, etc.);
- c. data errors (location on panel, quality of display, interpersonal communications);
- d. misleading data (cues match procedure, training in cue recognition, etc.);
- e. procedure format (visibility and salience of instructions, place-keeping aids);
- f. instructional clarity (standardized vocabulary, completeness of information, training provided);
- g. instructional complexity (use of "not" statements, complex use of "and" & "or" terms, etc.); and
- h. 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 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 application of the THERP method is not described in detail in the revised submission. However, the summary description indicates that the method was applied consistently with the THERP Handbook, NUREG/CR-1278³.

Compared with the method used in the original WCGS IPE submittal, it is considered that the CBDT method does provide a more realistic assessment of 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 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.

In a limited (though unspecified) number of cases, the cognitive portion of the human action was quantified using the THERP "annunciator model"--for example, the post-ATWS actions.

³NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, A.D. Swain & H.E. Guttman, Sandia National Laboratories, Albuquerque, NM, August 1983.

A.4 Summary of Results of Requantification

The overall effect of the requantification is to increase the contribution to the frequency of WCGS core damage from human actions. The licensee indicated that using the revised HRA values increased the total CDF approximately 24% over the frequency of $4.2\text{E-}5$ per reactor-year identified in the original submittal. The most significant increases in the probabilities of failure of human action events are shown in Table A-1, and the most significant decreases are shown in Table A-2.

In the revised submittal, the licensee has not provided an explicit analysis of the importance or relative contributions to the core-damage frequency of human actions. The two highest contributing sequences involving operator actions represent large LOCAs, with failure to implement low-pressure recirculation ($1.0\text{E-}6$ per year), and to recognize the need for low-pressure recirculation ($9.5\text{E-}7$ per year), respectively. Based on the highest ranked cutsets involving operator actions, other important human actions include OPA-OFB-EXE (failure to carry out feed-and-bleed actions), OPA-ECCSTRP2-COG and OPA-ECCSTRP2F-COG (failure to decide to trip high-pressure ECCS pumps on loss of cooling), and OPA-OD-EXE and OPA-EC3-EXE, failures to carry out RCS cooldown and depressurization actions following steam generator rupture.

It is noted that the sequence involving failures of operator to accomplish the "bleed" portion of feed-and-bleed cooling in the event of a steam-generator tube rupture (ranked 60th in the contributors to core damage frequency--sequence SGRS15, $5.3\text{E-}8$ per year) is a dominant contributor to the WCGS off-site releases.

Table A-1, Revised Human Failure Events with Significantly Increased Probabilities.

Event	Description	New HEP	Old HEP
OPA-OST	Failure to terminate HPI for SLB event	$1.2\text{E-}2$	$5.8\text{E-}5$
OPA-RCD2	Failure to perform RCS cooldown & depressurization	$1.4\text{E-}2$	$1.3\text{E-}4$
OPA-LTS	Failure to establish long-term heat removal	$1.8\text{E-}3$	$4.4\text{E-}5$
OPA-EC3	Failure to perform RCS cooldown & depressurization, SGR	$8.2\text{E-}3$	$2.2\text{E-}4$
OPA-MFW	Failure to restore main feedwater	$2.1\text{E-}2$	$6.0\text{E-}4$

Table A-2, Revised Human Failure Events with Significantly Decreased Probabilities.

Event	Description	New HEP	Old HEP
OPA-MRT	Failure to open RDMG input breakers manually	$1.0\text{E-}4$	$1.6\text{E-}1$
OPA-MSISOL	Failure to isolate BLDN after remote ISOL fails	$1.3\text{E-}4$	$4.0\text{E-}2$

OPA-MANUALRT	Failure to initiate manual reactor trip	1.0E-4	1.4E-2
OPA-LP1	Failure to establish low-pressure injection	1.9E-4	7.4E-3
OPA-NK020A	Failure to perform local actions of OFN NK-020	1.7E-3	5.6E-2

A.5 Observations

Based on the information provided, it would seem that the reanalysis of human actions has substantially removed most of the concerns expressed in the main portion of this report.

Specifically, the licensee has made the following changes to the WCGS 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. incorporation of an analysis of dependencies between human actions occurring in single cut-sets;
- iv. 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
- v. 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 which were developed from psychological models as described in Reference 2. The use of this method to quantify the decisionmaking element of the post-initiator actions therefore removes one of the major limitations of the WCGS HRA portion of the 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 WCGS 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 failures from the

9/05/96

actions not being completed in time. In addition to the actions associated with ATWS events (for example, OPA-MRT) where actions must be accomplished within 1 minute, there are a few "short-term" actions identified in the revised submittal, including switching over CCW service loops (action OPA-CCWSERLP, 5 minutes) and terminating HPI for a steam-line break event (action OPA-OST, 10 minutes) plus several required in the 15 to 20 minute time frame. All of these actions are performed in the control room, so access time is not a factor in taking time to perform the actions. However, several ex-control-room manual actions are required to be accomplished within a 30-minute time frame (for example, actions OPA-ALT, to establish alternate cooling and OPA-CCWHX, to close CCW heat-exchanger bypass valve). There is no indication that the time required to perform these actions is substantially less than the time available. For example, establishing alternate cooling paths can involve temporary interconnection of hoses to fire-pumps and, hence, can involve lengthy operator activities. While no information is provided concerning the importance of these actions to the WCGS core-damage frequency; action OPA-ALT does appear in several sequences with frequencies in the range of $1.8E-7$ per year and lower. Compared with other applications of the CBDT method, where operators have less than 1 minute to perform actions for scenarios other than ATWS, it is considered that a time of 5 minutes available to perform the actions entirely within the control room is a reasonable application of the method, though this time must be considered somewhat of a lower limit of the time available for the method.

The revised submittal does identify that dependencies between human actions were sought and modeled explicitly. First, in the case of post-initiator human actions, the cases where alternative task-execution actions depended on a single decisionmaking action were identified and modeled explicitly. Second, dependencies between initial failures and recovery actions were addressed. Finally, a review was performed of cutsets following the final sequence quantification to identify cases where multiple human actions were indicated; several cases were identified where additional dependence modeling is required, and the licensee intends to incorporate that modeling in a future revision. No details were provided for the ways in which the dependencies between failures and recovery actions were modeled, or how the future revisions will be performed.

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.