123 Main Street
White Plains, New York 10601
914 681 6846

New York Power
Authority

Ralph E. Beedle
Executive Vice President
Nuclear Generation

September 1, 1992
JPN-92-046

U.S. Nuclear Regulatory Commission
ATTN: Dccument Control Desk
Mail Station P1-137
Washington, D.C. 20555

SUBJECT: James A. FitzPatrick Nuclear Plant
Docket No. 50-333
Individual Plant Examination

References:

1. NRC letter, B.C. McCabe to NYPA, dated May 20, 1992, "Request For Additional Information Regarding Individual Plant Examination-James A. FitzPatrick Nuclear Power Plant."
2. NYPA letter, R.E. Beedle to NRC, JPN-91-048, dated September 13, 1991, providing the FitzPatrick IPE.
3. NRC Generic Letter 88-20"Individual Plant Examination for Severe Accident Vulnerabilities," dated November 23, 1988.

Dear Sir:

The Authority's response to the NRC request for additional information (Reference 1) regarding the Individual Plant Examination (IPE) for the James A. FitzPatrick Nuclear Power Plant is provided in the attachment. The NRC request was based on the review of the IPE report (Reference 2). The IPE was prepared in response to Generic Letter 88-20 in which the NRC requested all utilities to perform a systematic examination of the nuclear power plants to identify plant- specific features which may constitute a vulnerability to severe accidents.

Should you have any questions regarding this matter, please contact Mr. J.A. Gray, Jr.

Very truly yours,

Ralph E. Beedle

Attachment: as stated

cc: see next page

A011

cc: U.S. Nuclear Regulatory Commission
Region 1
475 Allendale Road
King of Prussia, PA. 19406

Office of the Resident Inspector
U.S. Nuclear Regulatory Commission
P.O. Box 136
Lycoming, NY 13093

Mr. Brian C. McCabe
Project Directorate I-1
Division of Reactor Projects-I/II
U.S. Nuclear Regulatory Commission
Mail Stop 14 B2
Washington, D.C. 20555

JAMES A. FITZPATRICK NUCLEAR POWER PLANT
INDIVIDUAL PLANT EXAMINATION (IPE)

RESPONSE TC
REQUEST FOR ADDITIONAL INFORMATION (TAC NO. M74411)

Item 1

Request

With regard to the peer-review process please provide:

(A) A summary of the in-house peer-review group findings, including recommended changes, and the disposition of recommendations. (NUREG-1335 notes the benefit of having the IPE reviewed in-house.)

(B) A listing of technical findings and recommendations of the three outside consultants that reviewed the IPE and a discussion of the disposition of any recommendations.

Response

The internal peer-review was performed in two stages. First, the methodology and guidelines document, individual system work packages (system descriptions, fault trees, and data), event trees, accident sequences, and other analyses were reviewed by cognizant operations, maintenance, technical services, instrumentation and control, licensing, and training staff both at the plant and in the head office departments supporting the plant. Second, an independent review team reviewed a draft of the IPE final report.

The review of individual work packages, etc., entailed the scrutiny of documents and plant site meetings to ensure the accuracy and adequacy of the models used. These reviews and meetings were an integral part of the information gathering process for the IPE. The consultations were comprehensive and conducted to the satisfaction of the authors of the IPE and plant and other Authority staff.

The formal in-house independent review of the draft IPE report was conducted by a review team comprising:

- Herschel Specter--Technical advisor to the Executive Vice President, Nuclear Generation (Chairman of the Review Committee)

  As chairman of the independent review committee, Mr. Specter coordinated the review and prepared a final report.

- George Wilverding--Manager, Nuclear Safety Evaluation; Chairman, Safety Review Committee (SRC)

  Mr. Wilverding focused on the comparison of JAF and Peach Bottom.

- Frank Pesce--Director, Quality Assurance

  Mr. Pesce's review addressed conformance with NRC guidelines for the development of the IPE.

- Verne Childs--Senior Nuclear Licensing Engineer, JAF

  Mr. Childs' review focused on ensuring the accurate portrayal of systems, operating procedures, plant response to initiating events, and subtle dependencies.

The comments made by each member of the review team will now be summarized together with the response of the authors of the IPE to them.

Herschel Specter (Technical dvisor to the Executive Vice President, Nuclear Generat)

The majority of Mr Specter's questions and comments were made to clarify statements made in the draft report:

- "....*(how can the 10^{-8}/year cut-off value for sequence development be reconciled with the 10^{-9} truncation value, excluding initiating event frequency, used in accident sequence quantification?)*..."

  The 10^{-8} cut-off value for sequence development was applied to sequences in which:

  - The probability of the first two or three events (including the initiating event) was <10^{-8}/year

  - Additional failure events with probabilities of 10^{-2} or less would have to occur to cause core damage.

  Therefore while the 10^{-8}/year was quoted to curtail discussion of accident sequences in the IPE report, the cut-off value used to stop sequence development was actually 10^{-10}/year or less. For example, sequences which entail a large LOCA (A) and loss of offsite power occasioned by random failures (B1) start with a probability of 6.73 x 10^{-9}/year (the product of 10^{-4}/year (A) and 6.73 x 10^{-5} (B1)). Because further events must be included in each sequence to cause core damage and these events have failure probabilities of 10^{-2} to 10^{-3}, sequences containing the events A and B1 were developed no further.

  The 10^{-9} sequence probability, excluding initiating event frequency, was the value used to truncate sequence quantification in the sequences developed.

- *"(..the assertion that 'if containment fails before core damage, a greater release of fission products to the environment occurs' is not always true. For example, if the failure occurred in the wetwell air space, the releases would be less than those resulting from drywell failure that occurred after reactor vessel failure)."*

  The report was modified appropriately.

- *"...query the validity of certain dominant SBO accident sequences."*

  These sequences were subsequently reevaluated with an additional emphasis on recovery actions.

- *"A decision to omit piping ruptures from system models cannot apply to breaks that initiate LOCAs."*

  A correction was made to the text.

Frank Pesce (Quality Assurance)

While Mr. Pesce and his colleagues found no specific deficiencies in the contents of the report, they did identify programmatic weaknesses in the documentation of internal reviews and the control of changes, software and records. The programmatic weaknesses are based on the assertion that the IPE should be treated as a safety-related document because of its use to support decisions relating to safety. However, the authors of the JAF IPE took the position that without a NRC-mandated formal record program with attendant quality program requirements, the retention of all documents essential to an audit required in Generic Letter 88-20 met all reasonable requirements[1]. Accordingly, no steps were taken to enhance documentation and control of changes, software and records.

George Wilverding (Manager, Nuclear Safety Evaluation)

Mr. Wilverding's comments were essentially editorial in nature.

Verne Childs (Senior Nuclear Licensing Engineer, JAF)

Mr Childs' review focused on the accuracy of the descriptions of systems, their functions, and behavior. For example, he pointed out that:

[1] These requirements are further detailed in NUREG-1407, "Procedure and Submittal Guidance for the Individual Plant Examination of External Events for Severe Accident Vulnerabilities," Appendix D, Pg D-4, Staff response to Question 1.5.

- Discharge of reactor coolant through the RHR heat exchanger tube sheet gasket was not a feasible V sequence (interface system LOCA).

- Success of high pressure coolant injection using RCIC with suction remaining on CST in small break LOCAs implied that RCIC provides reactor make-up during, rather than after, containment venting.

- The operator may be required to realign loads supplied by the 4.16-kV electric power system during full load testing of the EDGs as well as upon loss of a bus.

- The double 4.16-kV bus tie/isolation breakers connecting safeguard buses to their non-safety-related normal supplies trip before, rather than upon, closure of the EDG output breakers to prevent EDG overload and to separate the safety-related and nonsafety-related power distribution systems.

In addition to the internal peer-review, three outside experts also made a detailed review of a draft of the final IPE report. The experts were:

- Dr. Norman C. Rasmussen, McAfee Professor of Engineering, Massachusetts Institute Technology

  Professor Rasmussen provided an overview of the methodology, the application of fault and event tree analysis, and confirmation of the "reasonableness" of the results when examined both in isolation and in comparison with Peach Bottom.

- Dr. Gareth W. Parry, NUS Corporation

  Dr. Parry confirmed the adequacy and applicability of the accident sequences and reviewed the scope of the analysis of subtle dependencies and data.

- Dr. Alan D. Swain

  Dr. Swain validated the human reliability analysis described in the draft report with respect to its methodology and adequacy and the accuracy of results.

The comments of these reviewers can be summarized as follows.

Professor Norman C. Rasmussen

Professor Rasmussen summarized his comments by stating that he found the report to be "well laid out and clearly written. The essential information ... seems to all be there." He did, however, pose a number of questions and remark upon specific changes that he felt would be desirable. Most of these questions and changes were editorial in nature and the text of the IPE report was changed to address them. Other changes and questions were technical. These changes and questions and their resolution are as follows:

[1] *"Use of a 10^{-8} cut-off in the event sequences may cause concern unless you can show what is eliminated is much less (than) that what is kept."*

As noted in the response to Mr Specter's comment, a cut-off of $<10^{-10}$/year was used to curtail sequence development. In event sequence quantification, a sequence probability of 10^{-9} excluding initiating event frequency, was used for event sequence truncation. This cut off level ensured that the causes of at least 95 percent of the accident sequence frequency were computed.

[2] *"You eliminated floods (as a potential cause or contributor to core damage) but also suggested some changes to the plant to better cope with floods. This seems somewhat inconsistent."*

The internal flooding analysis did recommend that additional protection be provided to protect motor control centers BMCC1 (for RCIC) and BMCC2 (for HPCI) from spraying or splashing effects. These motor control centers are close to the stairways in the reactor building. This recommendation was retained as it provides a simple and inexpensive way to eliminate a potential minor contributor to causes of core damage at JAF, regardless of the fact that its risk significance is low.

[3] *"A core melt starts at 11 hrs. so it is not clear that electricity recovered in 11 hours will save the day. It seems to me that this may not be conservative... The probability of non-recovery of power is very important in determining (core damage frequency)."*

In the dominant sequences initiated by a loss of offsite power, recovery of offsite power was considered--a probability of 0.013 for the non-recovery of LOSP in 13 hours was included for requantification. This time allowed for HPCI failure on battery depletion after 8 hours and core damage after 13 hours. It was assumed that core cooling would be implemented rapidly after power recovery.

Dr.Gareth W. Parry

Dr. Parry in his summary of comments upon the IPE stated that "the project staff are to be complimented on the thoroughness of the analysis which will produce a high quality PRA. Because the team has done such a thorough job, I have relatively few comments to make that would significantly alter the results of the study, although I do feel the core damage frequency is a little low." Dr. Parry divided his comments into four main groups: accident sequence development, parameter estimation, sequence quantification and recovery analysis, and others. His non-editorial comments and their resolution follow.

Accident Sequence Development

[1] *"In the ATWS event trees, the need for blowdown to maintain pool temperature below the HCTL has not been addressed. The significance of depressurization is that it allows low pressure systems to inject. While there is an instruction to secure all injection other than SLC, CRD, and RCIC, if the operators forget a low pressure system such as condensate, they could after blowdown experience a sudden injection of cold water. This may not be a significant effect numerically, so I wouldn't change the trees right now. However, it is worth discussing with training/ operations to stress the need to think of the condensate systems. Condensate is picked out because it is (not) a safety system as such, and might be overlooked (and was in the case of one simulator exercise that was observed, although not at JAF)."*

Because of the low probability, the need for blowdown and securing a low pressure injection system was not addressed explicitly in the event trees. Furthermore, the Authority contends that the EOPs are clear and that level control procedures will mitigate any failure to secure the condensate system.

Parameter Estimates

[2] *"The battery failure rate assumed a mission time model rather than a standby failure rate."*

The fault tree model was changed to reflect the use of a standby failure rate.

[3] *"The failure rates for the diesel generator... as backed out from the CCF (common-cause failure) rates appear to be very low compared to other assessments (10^{-3} for fails to start, and 10^{-4} for fails to run). I think you ought to make sure that these are defendable."*

The probability of a common-cause failure of four diesel-generators to start was calculated as the product of a probability of 1.15 x 10^{-3} the plant-specific independent failure to start probability for a single diesel generator, and a beta factor of 0.038. The common-cause failure probability is therefore 4.37 x 10^{-5}. The probability of a common-cause failure to start four diesel-generators was calculated with a beta factor of 0.013; the common-cause failure probability is 1.5 x 10^{-5}. The beta factors were taken from NUREG/CR-4550, Volume 1, Revision 1, Table 6.2-1.

[4] *"The CCF analysis, using NUREG-1150 values for the common cause factors, is not a plant specific analysis. While the numbers that result appear in the right ballpark, the way the analysis was done does not give any insight into why CCFs at the plant have such low values. I would strongly recommend that, at some point, the staff should review the data on which these parameter estimates are based... concentrating on failure mechanisms and defenses to enable the project staff to give plant-specific reasons why the CCF probabilities are expected to be low."*

This issue is addressed in detail in the response to Item 13. In summary, the basic methodology employed in the common-cause failure analysis was that described in NUREG/CR-4550, Volume 1, Revision 1, Section 6 and is described in the JAF IPE, Volume 1, Section 3.2.3.3. To account for potential common cause failures, redundant components were systematically examined and potential common-cause failures were included in the system models at appropriate levels. Because no JAF plant-specific common-cause failure data were identified, beta factors from NUREG/CR-4550, Table 6.2-1 were used in the development of all common-cause failure probabilities except those for battery failures.

[5] *"The use of actual train/component maintenance unavailability rather than using values pooled across the system, gives rise to an unwarranted model asymmetry. What is done in the JAF PRA is not standard PSA practice."*

This issue is addressed in detail in the response to Item 8. In summary, if a train is rendered unavailable by the removal from service of certain components or subsystems within the train, then the unavailability of the train occasioned by tests and maintenance can be calculated as the sum of test and maintenance unavailabilities of the components or subsystems. Estimates of train level unavailabilities occasioned by test and maintenance were based on the daily plant status reports (DSRs) issued at JAF and supplemented by data from the plant logs and the maintenance work order packages. The Authority believes that the use of actual train data is appropriate because these data reflect real differences between trains.

Sequence Quantification and Recovery Analysis

[6] *"T1-33 (and others like it). The recovery action identified is recovery of offsite power to re-establish the condensate system as an injection source. Since the principal cutsets are associated with valve failures, manually opening these valves would be a more appropriate recovery action, given that it would take some time to restart the condensate systems."*

The possibility of recovery in accident sequences associated with valve failures was re-evaluated with credit taken for the manual opening of valves as a recovery action. This action is described in the JAF IPE, Volume 2, Section E3.3.1.

[7] *"There are many ATWS sequences with multiple recovery actions (that).. are treated as being independent... (However), these recovery actions.. are dependent."*

The ATWS tree was restructured such that failure to determine the need to inject SLC (event C1) would preclude any subsequent recovery associated with power control.

[8] *"Use of the 10^{-8} cutoff on sequences..I'm still a little concerned about losing some contribution to core damage frequency, since with the very large number of basic events, caused by a more detailed decomposition than used in more "standard" PRA component boundaries, the combinatorial factors could mount up."*

This concern is addressed in the response to Professor Rasmussen's comment [1].

Miscellaneous Items

[9] *"Some sensitivity studies would help. One that was identified was the use of a four hour rather than an eight hour depletion time under SBO conditions. The allocation of a zero probability to the chance of the depletion time being less than eight hours is too optimistic."*

Sensitivity studies were performed for station blackout and for human recovery events. For station blackout, the mean core damage frequency from internal causes is dominated by long-term station blackout sequences. This frequency was estimated assuming battery depletion in 8 hours and non-recovery of offsite power at 13 hours. To determine the sensitivity of internal core damage frequency to the battery depletion time, two analyses were performed. In these, the core damage frequency resulting from internal causes was recalculated assuming a) 4 hour battery depletion and non-recovery of offsite power at 8 hours and b) 6 hour battery depletion and non-recovery of offsite power at 11 hours. The results of these sensitivity analysis were presented in the JAF IPE, Volume 1, Table 3.3.6.9. It was concluded that the core damage frequency would rise from 1.92 x 10^{-6} to 2.56 x 10^{-6} /year if 4 hour battery depletion and non-recovery of offsite power at 8 hours were assumed.

[10] *"The distributions on certain basic event probabilities produce random samples with values greater than unity. Either use a distribution like beta, or a much smaller error factor to remove this unwanted, and unphysical, figment of the analysis."*

The few basic event probabilities with high means and error factor were treated as point estimates in uncertainty analysis to avoid errors.

[11] *"The treatment of the battery as a backup to loss of battery chargers in the D.C. fault trees should be looked at again. The mission time for the battery ought to be the average repair time for a charger or, if this time is longer than the depletion time, no credit should be taken."*

No credit was taken in SBO sequences for the possible repair of failed battery chargers.

Dr. Alan D. Swain

Dr. Swain's comments focused upon the human reliability assessment. Dr. Swain stated that his "initial impression is largely favorable... Obviously considerable thought has been given to the influence of potential human errors on the accident sequences evaluated. There seems to be considerably more information about the role of operators in this PRA than in others I have evaluated. One of the most impressive features of the HRA is the use of information from simulator exercises representing a large number of accident sequences analyzed in the PRA."

Dr Swain also noted that "...the primary HRA method and data bank used are those presented in NUREG/CR-4772, Accident Sequence Evaluation Program Human Reliability Analysis Procedure (ASEP HRAP). The use of this generic procedure is intended to provide more conservatism in an HRA than would be the case were use made of the more analytical methodology and data bank in NUREG/CR-1278, Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications. Thus, even though there might be some uncertainty or disagreement among HRA experts as to levels of dependence and other performance aspects assessed in the JAF PRA, there is built in conservatism, which, in my opinion, is desirable in a risk assessment."

The built-in conservatism associated with the ASEP HRAP is an important aspect of the HRA performed for the JAF IPE as it serves to allay concerns about the human error probabilities (HEPs) used.

Dr Swain asked mahy questions and made many comments. While some of these were essentially editorial or related to problems with traceability or the correction of small errors, others were of more technical import. The latter questions and comments and the Authority's response to them are as follows:

[1] *"In the Peach Bottom PRA, the published HRA included a reluctance factor of 2 for activation of SLC. In my separate, unpublished HRA I felt this assessment was inappropriate, based on interviews with trainers and operators."*

In the JAF IPE, the reluctance factor for operation of SLC was based on actual simulator experience and interviews with trainers and operators. As noted in the JAF IPE, Volume 2, Appendix E, Section E2.1.3, no reluctance to activate SLC was observed.

[2] *"Use of different crews for calibration of redundant channels is recommended. Is this policy followed at JAF? Was credit taken for such a policy? Is this explained somewhere? Reference here to some other section would be helpful."*

The schedule for the calibration of redundant channels at JAF is designed to ensure that they are calibrated at different times and by different crews. This schedule applies to instrument functional test and calibration of trip units and level and pressure switches, etc. Credit was taken in the IPE for the use of different crews to calibrate redundant channels.

[3] *"Have operators been training to use the firewater system as described, and does the EOP/AOP include this? Was PRA credit given for this possibility? In general, I usually take the position that without adequate practice of operator recovery functions, there should be no credit given in the PRA. I hope this is covered elsewhere in the report."*

The operators have been trained to use the fire water system to inject water into the core through the RHRSW A header as described in OP-13. This notwithstanding, no credit was taken in the JAF IPE for use of the firewater system.

[4] *"Do system responses include human performance? I note that human performance rarely appears in the system event trees beginning on p 3-15. This could be a cause for some criticism of the PRA. The tendency now is to put important operator terms into the system event trees, as was done in the Grand Gulf PRA. Perhaps the document could state a few words on this point about how human performance has been incorporated into the event trees. Perhaps the absence of human performance terms is more apparent than real."*

The event trees were modified to include human actions.

[5] *"Observations (on the performance of the various operating crews) are very useful in a qualitative sense and can be used as a basis to lower or raise the tabled HEPs in the ASEP HRAP. If this is what was done, some detailed description of such adjustments should be made so that it can be evaluated, i.e., so that what was done is traceable. One need not apologize for using such qualitative information to adjust estimated HEPs, but the procedure for doing so should be described."*

No specific rules were generated to apply these observations. Rather, observations were made to ensure that there were no deficiencies that would undermine the determination of HEPs. While the quality of the crews demonstrated in simulator exercises provides a strong basis for the HEPs derived using ASEP HRAP, the findings based on observations of their behavior in simulator exercises were used conservatively.

[6] *"Section 3.3.3.5, Pre-Accident HRA Results and associated tables: Traceability is inadequate at this point in the document. Where is the source, e.g., ASEP table number and item number? I think this should go in the table, as was done in the Grand Gulf HRA. There is no way I can evaluate these estimated HEPs without further information. Perhaps this information comes later in the report. If so, reference in Section 3.3.3.5 should be made to the appropriate place. (As I later discovered, the HRA document does not include this necessary information.)"*

A new table for the pre-accident results was constructed and an introduction describing the table was provided for Section 3.3.3.5. Subsequently, Dr Swain wrote "I did review each HEP calculation, assuming that the claims for recovery factors and the number of activities assessed were indeed correct, and that these claims can be substantiated in a clearer and more detailed description of the underlying human activities for the task assessed. I found each arithmetic calculation to be correct, but I emphasize this is only a check on the arithmetic."

[7] *"HEP (for miscalibration of steam line high flow transmitters) is questionable. There appear to be some possible misapplications of the pre-accident assessment rules from the ASEP HRAP. If the following problems are only the result of inadequate written communication, and the assessment of recovery factors and number of critical actions is correct, then the assessed HEP is OK. At the very least, considerably more explanation is needed.*

a. *Under "ACTIVITIES," it looks like Activity C has two critical actions while Activity D has a different two critical actions. Isn't it true that any one or more of the four "adjustments" would be considered a failure? If so, the equation for the NHEP for 23DPT-76 would have a multiplier of 4 rather than 2, an increase in NHEP by a factor of 2.*

b. *The terms used in Activities C and D confuse me: "adjust zero adjust," "adjust zero," and "adjust span adjust," which is used twice.*

c. *Under "DEPENDENCY," item (1) implies to me that Activity C applies to one component (e.g., 23DPT-76) while Activity D applies to the other component (e.g., 23DPT-77). But in item (2) it states that there is only one component. Very confusing language.*

d. *Under "RECOVERY," para 1 appears to be claiming too many recovery factors.*

1) *First, there is no description of the activity involved in Step 5.3.3.4 or in Step 5.4.3.4 which are supposed to "verify" that the two separate steps in Activity C and the two steps in Activity D were carried out correctly. What does "verify" mean? Is some kind of real test conducted, or does the original performer just look at some displays to see what the values are? I do not give any recovery credit for one person checking his own activities unless these checking activities are separated from the original activities in both time and space. I would need more description of what takes place before allowing any credit at all.*

2) *Second, even if it were valid to allow credit for*

Optimum Condition #2 (the PC test), it does not seem correct to also allow credit for Optimum Condition #3. This smacks of double credit, in my opinion. Also it does appear that the "different time and place" requirement of T5-1 #4c(2) is not met. In short, I fail to see any rationale for any recovery credit from Optimum Conditions #2 and #3. Obviously, some clarification is needed here.

e. *Paragraph 3 under "RECOVERY," claims credit for a daily check (Optimum Condition #4). No mention is made of the use of a written checkoff list per T5-1 #4d. If such a list were used for all daily checks, this information could be stated once in the introductory information related to the pre-accident HRA. Based on oral information from Ms. Drouin, I shall assume that a written checkoff list is used.*

f. *If Optimum Condition #3 is not correct, but Optimum Conditions #2 and #4 are correct, the result is Case IX in T5-3. For this case, the HEF would be identical to the HEP assessed. If only Optimum Condition #4 is correct, the HEP would have to be increased.*

g. *It would be helpful to a reviewer to include the correct Case number from ASEP HRAP Table 5-3 in the section on "RECOVERY" in the HRA for each HEP."*

The Authority's response to each item raised is as follows:

a. In both cases the tasks are highly related and constitute one step in the written procedures. Thus, complete dependence was assumed.

b. This terminology is used in the procedure.

c. The activities apply to each of the components.

d. 1. Admittedly this was confusing, but the post-calibration check is an actual calibration test directed by the procedure.

   2. The verification task ensures that the restoration of the component is complete and it is checked-off (written check list) by a second individual. In addition, there are several indicators in the control room that must clear after restoration and these are also checked.

e. A written check-off list is used.

f. The HEP is correct.

g. RFs applied to each step or component were included in tables.

Finally, Dr Swain noted that "The equation for the total NHEP in which any error on the calibration of one component is assumed to carry over to the second component provides conservatism, which many reviewers would find laudable."

[8] *"Are the JAF ROs (reactor operators) required to memorize the entry conditions for the 10 JAF EOPs? If so, how often are they tested to ensure that they really have memorized the entry conditions? I note that the first entry in Table 3.3.3.2 assesses a negligible <1E-5 HEP for entering the wrong EOP. Required memorization and frequent testing could provide a rationale for this HEP. Otherwise, why should a reviewer believe the <1E-5?"*

Operators at JAF are required to memorize the entry conditions to the EOPs and practice them at least monthly during simulator exercises.

[9] *"Another concern is the appearance of an arbitrary use of a factor of 5 or a factor of 10 reduction in the nominal HEPs obtained through use of the methodology and data base in NUREG/CR-4772, Accident Sequence Evaluation Program Human Reliability Analysis Procedure (ASEP HRAP). There are two points to be made here. First, insufficient rationale was sometimes provided to justify a reduction in the nominal HEP. Second, the ASEP HRAP itself provides for use of lower bounds of nominal HEPs if sufficient justification is provided."*

While not strictly in keeping with the ASEP HRAP methodology, reduction of nominal HEPs by factors of 5 or 10 was not arbitrary. Lower bound values and recovery credits in the ASEP HRAP methodology generally result in reductions by factors of 5 or 10. In situations where the HEPs generated with ASEP HRAP resulted in values that seemed overly conservative given the circumstances in which the human action is expected to occur, judgement was used to determine the reduction factor. Reductions were based on such aspects as the simplicity of accident conditions, quality of the EOPs with regard to the accident conditions, operator training and familiarity with the accident scenario, the decision and response time available, criticality of the action under consideration, and crew performance during simulator exercises. These issues were addressed in the introduction to Appendix E of the JAF IPE, Volume 2, and each reduction was explicitly justified at the appropriate place in the text.

[10] *"Another concern was inappropriate use of Table 8-5 in the ASEP HRAP. In several cases, seemingly independent (or at least not fully dependent) human actions were assessed as the equivalent of one action, and a single HEP was assessed for the entire set of actions. This simplification could lead to optimistic estimates of critical HEPs. This problem is mitigated to some extent by the fact that the generic HEPs in Table 8-5 are deliberately conservative.*

Part of this problem, at least for me as the reviewer, was the lack of sufficient documentation, especially drawings, information on specific training and practice provisions of critical tasks, minimum control room staffing and estimated times of arrival of other personnel after the initiation of some accident sequence, and so on, as described more fully in the attachment to this letter.

Ms. Drouin and her staff will make a more detailed evaluation of what does constitute a set of completely dependent actions, and re-assess the resultant HEPs accordingly. We went over a few of the operator actions involved, and it was apparent to me that some grouping of actions would indeed be appropriate. It would also be most inappropriate, and grossly pessimistic, to consider each action to be completely independent, and assign a nominal ASEP HEP of 2E-2 to each such action."

The resolution of what constitutes a completely dependent set of actions is not easy. The approach taken in the JAF IPE was to group actions and consider them dependent if the actions were "spelled out" in a logical sequence in a written procedure and if the actions were to be carried out to achieve a single goal. Other factors considered in determining whether complete dependence existed in a set of actions were whether operators will double check the procedural actions, the simplicity of the actions and procedure being followed, the time available, and the apparent understanding of the procedure demonstrated by the operators during the plant walkthroughs. During discussions with Dr. Swain, agreement was not always reached concerning which actions should be considered dependent. Where disagreements existed, justification for our position was provided in the JAF IPE.

[11] *"The treatment of error factors (EFs) is not that recommended in NUREG/CR-4772, the ASEP HRAP. It is stated that "In general, if the desired HEP was a composite of several HEPs, the error factor selected was that associated with the dominant HEP." The ASEP HRAP provides a computer program for propagating the error bounds through an HRA event tree consisting of more than one HEP. The JAF method would result in a final EF than would be smaller than the EF*

derived by propagating the EF associated with each HEP in some set of actions. Frankly, this does not really bother me, as I think too much has been made of error bounds. Given the generic nature of the HEPs in the ASEP HRAP, the associated EFs are not to be considered accurate estimates. In my work in HRA I preferred merely to use the median HEPs. With the data available for estimating HEPs, the careful statistical treatment of EFs provides verisimilitude that is most inappropriate."

Final EFs were determined as described in the text. The Authority agrees with Dr. Swain's comments regarding EFs and chose not to use the computer program for propagating error bounds.

[12] "*E2.1.2: I cannot tell from the document which operator is involved and what and where the displays are located. SAIC information indicates the RO is normally near Panel 09-5. I agree that "failure to diagnose" can be ignored. However, if NUREG/CR-4772 is being used as the HRA procedure and data base, rather than <1E 5 for failing to verify and initiate ARI and RPT and to override ADS, it would be more appropriate to assess the HEP for these immediate actions from T8-1 #9f and T8-5 #10 (my shorthand notation for Table 8-1, item #9f, and Table 8-5, item #10), and use 1E-3 as the nominal HEP. Then if one can justify (in the document) the use of the lower bound, the revised HEP would be 1E-4. In general, if one is using the ASEP HRA Procedure, rather than simply make some untabled (sic) estimate, it is preferable to refer to some ASEP HRAP table and item number and make appropriate adjustments from that starting point."*

In the JAF IPE, Volume 2, Appendix E, it was noted that when an HEP was determined to be negligible, it was assigned a value of "<10^{-5}" and the "<" sign was dropped for systems analysis purposes. ASEP HRAP allows the assignment of "negligible" HEPs in some circumstances, e.g., Table 8-1, item g. A negligible probability of failure is traditionally assigned a value of 10^{-5} and the differences in "negligible" do not seem critical. Thus, the values were not changed.

[13] "*E2.2.5.2: I assume that AOP-37 has each of the steps in this lengthy procedure fully documented. If not, the assumption of a step-by-step task would be inappropriate. The taking of time measurements in a simulation of the task is obviously far superior to taking someone's time estimates. My problom here is the assessment of just one HEP for the entire task consisting of many apparently critical actions. I see many opportunities for errors of*

omission. If the task is not practiced, errors of commission could also occur. Without more familiarity with this task, all I can say is that I believe the assignment of a single HEP for all the critical actions taken together is probably too optimistic. I cannot agree with the HEP. Note the first footnote in T8-5 which states, "The HEPs are for independent actions or independent sets of actions in which the actions making up the set can be judged to be completely dependent..." The assessment of one HEP is equivalent to saying that if one of the many actions is done, the others will all be done. To me, this is not credible. I would probably not think it reasonable to assess a .02 HEP for each critical action; there are bound to be some RFs and dependencies. But with the information I have, I cannot make a realistic assessment."

The Authority elected to stay with the assumption that all the actions were dependent. The general reasons for making such an assumption are described in item [10] above. Furthermore, while the times listed for task performance in the report are single operator times, a second operator would be double checking the performance and could assist in carrying out the actions. In addition, a maintenance crew would also be available. Given that the steps are clearly spelled out in the procedure and the fact that during the plant walkthroughs a reactor operator who had only been licensed for two days was found to be completely familiar with the procedure, it was felt that complete dependence was justified.

[14] *"E2.3.5.1: Following is my original evaluation, which was based in part on a misunderstanding of the accident sequence: "It is difficult for me to try to evaluate the level of stress involved if things get so bad that depressurization is required. Obviously, the analysts assumed only a moderately-high stress level. I think more justification is needed for that assessment, especially in view of the use of the lower bound diagnosis HEPs assessed. My strong impression is that the assessment is unduly optimistic." My misunderstanding indicates that further information and justification is needed in the text.*

Mary Drouin pointed out that long before Emergency Depressurization would be required, the crew would have been trying to maintain level with all systems available. And with the accident sequences being assessed, the need for rapid, full emergency depressurization would not likely occur. I think this could be made clearer in both Figure E2.15 (p E-47) and in the related text. It seems to me that two analyses could be made to assess: (1) the probability that the full-scale, rapid depressurization would have to be done, and (2) given (1), the probability that it would not be accomplished. Moderately-high stress would be appropriate to (1), and extremely-high stress might well be appropriate to (2).

Regardless of what is done, I still find no good justification for using the lower bound HEPs from Figure 8-1 in the ASEP HRAP."

The Authority contends that all operators are particularly aware of the fact that they must depressurize to use the low pressure systems. In addition, they are trained extensively to do this when the appropriate situation arises. Thus, the lower bound was felt to be appropriate.

[15] "*E3.3.1.1: I disagree with the first sentence. To me, this is analogous to a statement made by an NRC person at a meeting of HRA specialists. He stated unequivocally that it does not matter how many annunciators are screaming for the operators' attention. He believed that the operators will simply ignore those that are not relevant to the situation and concentrate on those that are relevant. Para 1 in E3.3.1.1 explains away all problems. I find it not to be a credible statement. If we are talking about a large LOCA, remember that an extremely-high stress level is assessed from t = 0.*

In discussions with Mary Drouin, she strongly believes that my assessment of extremely-high stress for a Large LOCA is no longer appropriate so many years after WASH-1400. This is obviously a judgment call. I prefer to stick with the extremely-high stress assessment. A large LOCA is never, I repeat, never anticipated. "It just cannot happen here." In my judgment, the incredulity effect will be great."

The Authority believes that there are enough cues available for the crew to determine that a problem exists. Our experience with operating crews is that they attempt to diagnose problems and in this situation there are simple cues available and 50 minutes are available for the diagnosis. Furthermore, extremely high stress was assessed for the LOCA case.

[16] "*E3.4.1.2: The nominal HEP of .02 seems OK, but the factor of 10 reduction is not adequately justified. At the most, from the description of skill levels involved in this task, only a factor of 5 reduction can be assessed per the ASEP HRAP.*"

This is clearly a matter of judgement. However, given the simplicity of the task and the training the operators receive to make sure the task is accomplished, the reduction of 10 was felt to be appropriate.

[17] *"E3.6.1.1: The argument seems reasonable, but the diagnosis median HEP for 660 minutes in F8-1 is about 2E-5 rather than 1E-5."*

Dr. Swain is correct. The HEP was changed

[18] *"E3.6.1.2: The assessment of task type and stress level seem appropriate, but the use of a single HEP for the combination of several actions is not given an adequate rationale. Read the first footnote in T8-5."*

This task requires the operator to open or close a valve or breaker. With only one or two things to do, dependence seems appropriate. In addition, with up to 11 hours available, there is likely to be plenty of time to recognize any problems. However, because the actions are performed outside the control room, no credit was given for a second check. Accordingly, the 0.02 value used is conservative.

Finally, in summarizing the technical findings and recommendations made in the peer-review process, it should be noted that all members of the review team stated that they did not expect any of these comments to result in a major change to the predictions and conclusions of the JAF IPE.

Item 2

Request

Discuss the treatment of plant-specific design and operational provisions that assure the long term makeup capability to the condensate storage tank (CST) in order to achieve the successful long term operation of the High Pressure Coolant Injection (HPCI) system or the Reactor Core Isolation Cooling (RCIC) system (after its suction switched back to the CST from the suppression pool) and the long term Control Rod Drive (CRD) injection to the reactor vessel during the containment venting scenario.

Response

The ability to provide long-term make-up to the CST will be challenged in sequences initiated by a LOCA in which containment venting occurs. However, only in small-break LOCA sequences is this of concern: the predicted frequency of sequences initiated by large and intermediate LOCAs in which containment venting occurs is below the 10^{-6}/year cut-off frequency identified by the Authority.

A small, 1-in. break, LOCA will result in CST depletion in approximately 22 hours, at which time make-up to the CST is required. The make-up capability is provided by the demineralized water storage and transfer system and is addressed in plant operating procedures F-OP-6/7/25. These procedures identify the steps by which water is transferred to the CRD system and CST--successful implementation of the procedures by plant operators will assure continued make-up to the CRD system and CST.

For sequences not initiated by a LOCA, thermal-hydraulic calculations performed using the MARCH computer code predict that make-up is not required during containment venting for operation of the HPCI, RCIC, or CRD systems within the 24 hour-mission time--CST depletion is predicted to occur after 44 hours.

Item 3

Request

With regard to the treatment of internal flooding, discuss the IPE's assessment of failure of the check valves located inside the drain system between two independent rooms having independent safety components.

Response

The potential common-cause failure of ECCS equipment caused by backflow through a stuck-open check valve in the equipment and floor drain system was addressed in the IPE. The issue is discussed in the JAF IPE, Volume II, Appendix H, page H-74. In summary, the analysis of this potential problem was performed in response to Information Notice No. 83-44, Supplement 1 (August 30, 1990) issued by the NRC. The analysis concluded that backflow from a flooded east crescent into the west crescent would have to persist for 2 hr 4 min. before redundant ECCS equipment is damaged and that backflow from a flooded west crescent into the east crescent would have to persist for 3 hr 33 min. before redundant ECCS equipment is damaged. It is highly probable that flooding within the crescents would be detected and stopped before damage occurred--annunciators would alarm at panel 09-4 in the control room on a high water level in the reactor building sump. Accordingly, the probability of damage to ECCS equipment as a result of backflow through the equipment and floor drain systems was considered negligible.

Item 4

Request

Provide a concise discussion of the IPE's treatment of Power Conversion System (PCS) recovery (if it would have been lost during the initial 30 minute period of the transient). Include in this discussion the dependency information between the condenser and the reopening of the MSIVs and bypass valves.

Response

No credit was taken for PCS recovery during the first 30 minutes of a transient. PCS recovery was considered only for those transients which progressed to long-term loss of containment heat removal accident sequences (TW sequences). Table 3.4.1.1 of the JAF IPE (pages 3-472 to 3-487) lists transients in which recovery of systems, components and operator actions was considered. The possibility of PCS recovery was considered in 19 sequences:

PCS recovery within 10 hours

T2-13
T3A-2-T2-13
T3A-3-T1-12

PCS recovery within 24 hours

T2-4
T2-17
T2-21
T2-40-T3C-5
T2-40-T3C-27
T2-41-S1-7
T3A-2-T2-4
T3A-2-T2-17
T3A-2-T2-40-T3C-5
T3A-2-T2-40-T3C-27
T3A-2-T2-40-T3C-33
T3A-3-T1-4
T3B-9-T2-4
T3B-9-T2-40-T3C-5
T3C-5
T3C-27

The probabilities of non-recovery of the PCS within 10 hours and 24 hours are 0.06 and 0.007, respectively. These data were excerpted from NUREG/CR-4550, Volume 1, Revision 1, Table 8.2-10 and are presented in the JAF IPE, Volume II, Section E3.2, pages E-59 and E-60.

The dependency between the restoration of condenser vacuum and the reopening of the MSIVs and bypass valves is addressed in the following plant procedures:

OP-1:	Main Steam System
OP-9:	Main Turbine
OP-24C:	Condenser Air Removal
AOP-15:	Recovery from an Isolation
AOP-31:	Loss of Condenser Vacuum.

Item 5

Request

Provide a concise discussion of recovery of failed Residual Heat Removal (RHR) pumps, Residual Heat Removal Service Water (RHRSW) pumps, and Core Spray (CS) pumps due to common cause failures as documented in Table 3.3.4.1 of the IPE. Include in this discussion the mission time versus recovery time involved for injection and long term decay heat removal, and the availability of overriding equipment involved, if any.

Response

In the JAF IPE, no credit was taken for the recovery of failed RHR, RHRSW and core spray pumps where failure is occasioned by common-cause failures. Credit was taken, however, for restoring RHR and RHRSW pumps in specific cut sets derived for accident sequences initiated by the loss of ac buses 10500/10600 or battery control boards BCB-A/B and accompanied by a loss of containment heat removal. In these cut sets, one set of pumps fail because of the loss-of-power initiator and other pumps are unavailable because of post-maintenance restoration errors. In these sequences, the operators would have 11 hours in which to diagnose the possible need to restore RHR and RHRSW pumps. The recovery actions are discussed in the JAF IPE, Volume II, Appendix E, Section E3.6, page E-69.

Item 6

Request

Discuss the treatment of DC load shedding, if needed, following a station blackout scenario, or loss of AC buses 10500 and 10600 scenarios. Does Fitzpatrick take credit for additional batteries for long term HPCI and RCIC initiation and controls to avoid a core damage event? If so, please describe treatment and justification for credit.

Response

In the event of a station blackout or loss of 4.16-kV buses 10500 and 10600, operators follow Abnormal Operating Procedures F-AOP-18/19/49 for loss of buses 10500, 10600 and station blackout, respectively. In procedure F-AOP-49, operators are specifically directed to shed dc loads to extend battery life:

- The dc-powered lube oil pumps for both reactor feed pump turbines, the main turbine, both recirculation motor-generator sets, and the main generator seal oil pump are secured.

- Various emergency lighting panels in the administration building, screenwell house, reactor building, heater bay, radwaste building, and the turbine building electric bay are either de-energized for the duration of the event or energized on an as-needed basis only.

- The uninterruptible power supply motor-generator set is tripped after one hour into the event.

In procedures F-AOP-18/19, operators are directed to monitor station battery charge and remove dc-loads as necessary to prevent excess discharge.

To ensure the most pessimistic battery capacity situation was addressed, the JAF IPE took no credit for dc load shedding until 30 minutes had elapsed from the start of the station blackout. This delay accommodates the time required for the operators to diagnose the problem and attempt restoration of ac power.

HPCI and RCIC were assumed to become unavailable upon station battery depletion. No credit was taken for use of alternate sources of dc and ac power such as the LPCI independent power supply system 419-V batteries and inverters because the use of these power sources to prolong station battery life is not addressed in any procedure.

Item 7

Request

Provide a summary discussion of the process used to address pressurization of the wetwell air space following a postulated pipe break event (subsequent to a successful scram or fail-to-scram event) in the Safety Relief Valve (SRV) discharge piping.

Response

The SRV discharge pipes are used only following transients accompanied by the loss of the condenser as a heat sink. In the course of these events, the discharge pipes can break because of nonmechanistic failures or water hammer effects--should an SRV cycle successfully but the SRV discharge line vacuum breaker fail to open, water will be drawn from the torus into the discharge line causing a water hammer and possibly discharge pipe rupture. Should the discharge pipes break in the wetwell air space, the wetwell will be overpressurized if the SRV on the failed line sticks open and if wetwell pressure is not reduced--intermittent discharges will not challenge wetwell integrity. Wetwell pressure will be reduced by operation of the torus sprays or by operation of the wetwell-to-drywell vacuum breakers and initiation of the drywell sprays.

The probabilities of event sequences that result in overpressurization of the wetwell were calculated. For nonmechanistic failures, a median pipe break probability of 10^{-9}/hr/100 ft of pipe was assumed. This value was taken from WASH-1400 and applies to high energy piping in continuous use[2]. Accepting this failure rate, the mean probability of nonmechanistic discharge pipe rupture is 2.04×10^{-7} for the assumed 24-hour mission time.

For a transient followed by a scram, discharge pipe rupture, and operation of three of the five vacuum breakers, the probability of wetwell overpressurization can be calculated as follows:

Event	Mean Probability
Reactor scram with condenser unavailable (T1+T2)	0.650/year
SRV discharge pipe rupture	2.04×10^{-7}
Stuck-open SRV on failed line	0.102

[2] In practice, because the discharge pipes are open to the torus, a leak-before-break failure mechanism is more likely than the double-ended guillotine break required to rapidly pressurize the wetwell air space. NUREG/CR-4792 indicates that the probability of the double-ended guillotine break is significantly less than that of a leak-before-break failure.

Operator failure to initiate torus or drywell sprays	2.6×10^{-4}

The resulting sequence probability is 2.5 x 10^{-12}/year, a probability that falls below the 10^{-8}/yr screening criterion adopted by the Authority for the elimination of sequences.

Should three of the five vacuum breakers fail, the probability of wetwell overpressurization will be reduced by a factor of 10^{-4}.

Should discharge pipe failure be caused by water hammer, the probability of wetwell overpressurization can be calculated as follows:

Event	Mean Probability
Reactor scram with condenser unavailable (T1+T2)	0.650/yaar
SRV discharge line vacuum breaker fails to open on demand	10^{-4}
Conditional probability of water hammer-induced pipe rupture	0.1
Stuck-open SRV on failed line	0.102
Operator failure to initiate torus or drywell sprays	2.6×10^{-4}

The resulting sequence probability is 1.7×10^{-10}/yr. This probability falls below the 10^{-8}/yr screening criterion and accordingly was eliminated from consideration.

Pipe rupture subsequent to ATWS events will be of even less concern because of the lower probabilities of these initiating events--the probability of ATWS events is <10^{-4}/year.

Item 8

Request

Describe the process used to estimate train level unavailability due to test and maintenance and human errors. Discuss the estimation of these components of train level unavailability for the Electrical System (transformer and inverters) and RHR System (injection mode, spray mode, pool cooling mode and shutdown cooling mode) as examples of the application of the above process.

Response

If a train is rendered unavailable by the removal from service of certain components or subsystems within the train, then the unavailability of the train occasioned by tests and maintenance can be calculated as the sum of test and maintenance unavailabilities of the components or subsystems.

Estimates of train level unavailabilities occasioned by test and maintenance were based on the daily plant status reports (DSRs) issued at JAF supplemented by data from the plant logs and the maintenance work order packages. The DSRs list all systems and components unavailable on a given day, but, because they do not distinguish between test and maintenance unavailability, no distinction was made between them in the data used. The use of plant data in estimating unavailabilities is described in the JAF IPE, Volume 2, Appendices B and D.

Electrical system unavailabilities (i.e., the unavailabilities of 115-kV lines 3 and 4 and station transformers 71T-2 and 71T-3 described by basic events ACO-MAI-MA-115K3, ACO-MAI-MA-115K4, ACO-MAI-MA-XFRT2, and ACO-MAI-MA-XFRT3, respectively) were calculated from the actual component/system out-of-service hours. The unavailabilities of transformers 71T-2 and 71T-3 were addressed separately from line unavailabilities because the transformers can be fed from either 115-kV line.

RHR system unavailability was estimated from out-of-service hours recorded for each component in the DSRs and other sources of plant data. The RHR system has two trains each of which has two pumps. Train and pump unavailabilities were depicted in the mutually exclusive basic events RHR-MAI-MA-LOOPA, RHR-MAI-MA-LOOPB, and LCI-MAI-MA-RP-3A/B/C/D.

In addition to these six basic events describing RHR system unavailability, six other basic events depict the unavailability of equipment in the three different modes of RHR operation modeled: the low pressure coolant injection mode (basic events RHR-MAI-MA-LPCIA and RHR-MAI-MA-LPCIB), the suppression pool cooling mode (basic events RHR-MAI-MA-SPCLA and RHR-MAI-MA-

SPCLB), and the containment spray mode (basic events RHR-MAI-MA-CSLPA and RHR-MAI-MA-CSLPB). The shutdown cooling mode of RHR operation was not modeled in the JAF IPE. Component out-of-service hours were assigned to these unavailability events based on component usage in the various modes of operation. The allocation of components to the various unavailability events is depicted in Figures 8.1 and 8.2.

The unavailability events were incorporated in the system fault trees as appropriate. For example, in the depiction of RHR/LPCI mode maintenance unavailability, the unavailability of train A in the maintenance mode was represented by three events (Figure 8.3): the unavailability of components in loop A (RHR-MAI-MA-LOOPA); the unavailability of valves in the LPCI injection path (RHR-MAI-MA-LPCIA); and the unavailability of pumps P-3A and P-3C and their associated equipment. The unavailability of pumps P-3A and P-3C is represented by an AND gate with basic events LCI-MDP-MA-RP-3A and LCI-MDP-RP-3C as inputs. It will be noted that maintenance unavailability events are not duplicated. Maintenance that would violate technical specifications (e.g., the simultaneous unavailability of both RHR trains) was eliminated from the cut sets during sequence quantification.

Unavailabilities occasioned by human error in tests and maintenance were estimated in a pre-accident human reliability analysis (HRA) that identified the appropriate man-machine interfaces and assigned nominal human error probability (NHEPs) to the selected tasks using the ASEP-HRAP methodology (NUREG/CR-4772)[3]. The pre-accident human error events are associated with the restoration of components to their proper positions or configuration after tests or maintenance. The first step in assigning NHEPs is to identify the critical human activities where errors may occur; these activities are then addressed in the system models. Examples of such activities are the restoration of a core spray pump to its normal operating condition after maintenance or calibration of a pressure transmitter. Once these activities had been identified, they were assigned a basic human error probability (BHEP) of 0.03. This BHEP represents a combination of a generic HEP of 0.02 for an error of omission and a generic HEP of 0.01 for an error of commission, with the conservative assumption that an error of commission is always possible if an error of omission does not occur.

The next steps involve identifying recovery factors (RFs) and dependence effects that influence the probability of human error. Dependence effects are important when the probability of success (or failure) in one activity depends on whether success or

[3] Alan Swain, "Accident Sequence Evaluation Program--Human Reliability Analysis Procedure," Prepared by Sandia National Laboratories for the U.S. Nuclear Regulatory Commission, NUREG/CR-4772, February 1987.

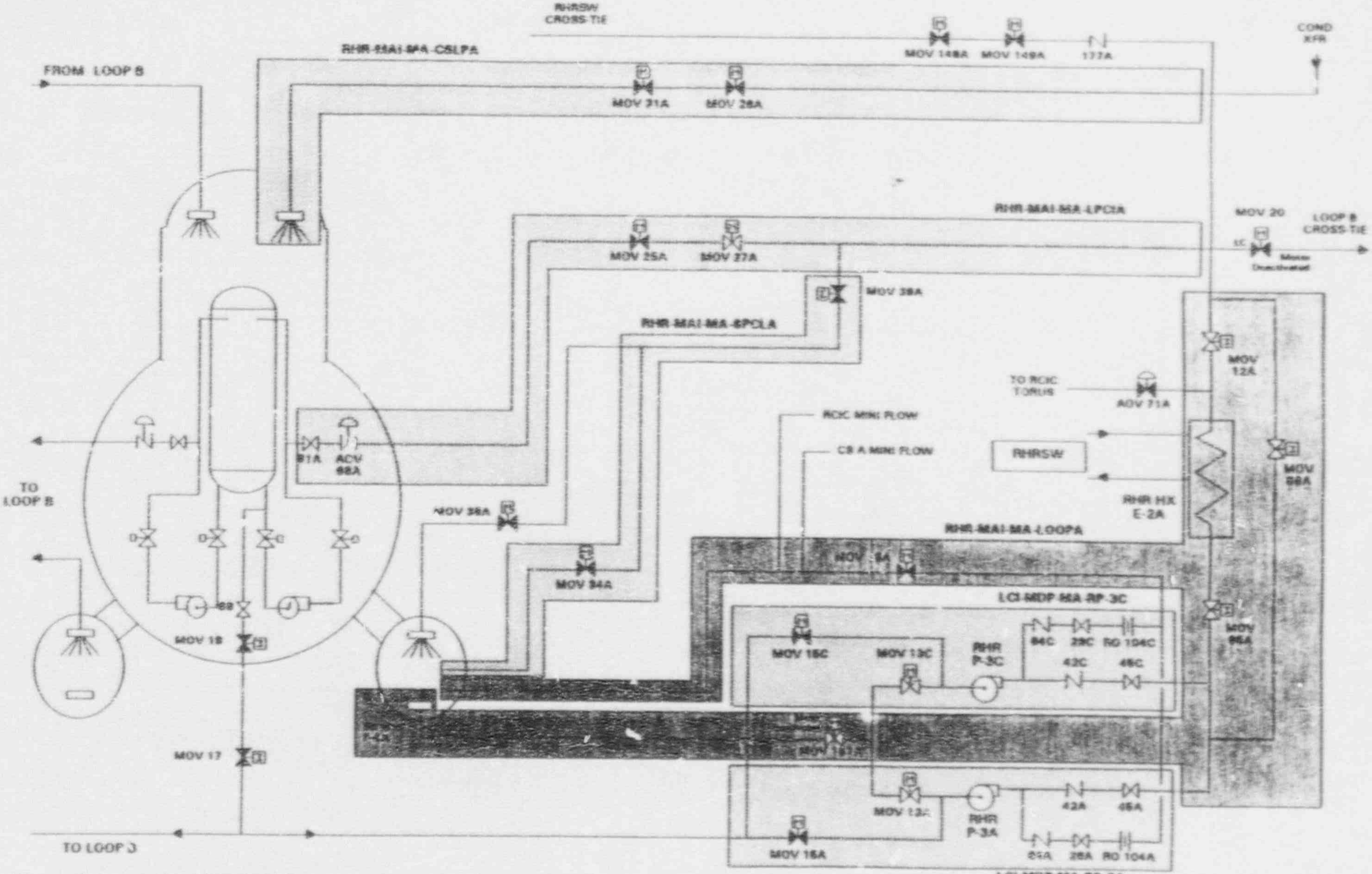
failure has occurred in another. Four factors were considered in determining whether dependencies existed in various operator actions: the number of components to be restored, the component configurations (series or parallel), the relative restoration time, and the relative location of the components to be restored. Only zero and complete dependence were considered in the JAF IPE.

RFs limit the undesirable consequences of human error by allowing for human redundancy, for compelling signals that notify operators of an unavailable component, for post-maintenance or post-calibration tests, and for frequent checks and inspections. The RFs applied to each step of a task allowed credit to be taken for post-maintenance or post-calibration check requirements, for verification in which a second person directly verifies component status or the original task performer verifies component status later at a different place from the original verification provided a written check-off list is used during the check, and for a check of component status made each shift or day if a written check-off list is used. Both dependence effects and RFs must be considered to obtain more realistic estimates of HEPs.

Once the appropriate RFs and dependence effects were identified, pre-accident NHEPs were determined by adjusting the BHEPs of the critical activities to reflect dependence effects and RFs. For example, if the procedure involved in calibrating a pressure transmitter demanded a post-calibration test and written verification of the test by another person, the BHEP of 0.03 would be adjusted by a factor of 0.01, resulting in an NHEP of 0.0003. Once the NHEPs were obtained, they were incorporated directly into the system fault trees. The handling of restoration errors is described in more detail in the JAF IPE, Volume 1, Section 3.3.3.

For the RHR system, restoration errors were modeled for each pump in basic events LCI-XHE-RE-PM3AP, LCI-XHE-RE-PM3BP, LCI-XHE-RE-PM3CP, and LCI-XHE-RE-PM3DP. Five components were modeled for each pump: pump, suction valves 10-MOV-13x and 10-MOV-15x, discharge valve RHR-45x, and manual minimum flow valve RHR-28x. A failure to restore any of these five components will cause RHR pump unavailability.

The probability of failing to restore 125-Vdc charger breakers (basic events DC1-XHE-RE-CHGAD and DC1-XHE-RE-CHGBD) was estimated in a similar manner. A failure to restore these breakers after tests and maintenance will result in a failure of the chargers to charge the station batteries and eventual battery depletion.



Note: Valves are shown in their standby position.

Figure 8.1 RHR System Loop A Component Maintenance Unavailability Allocation

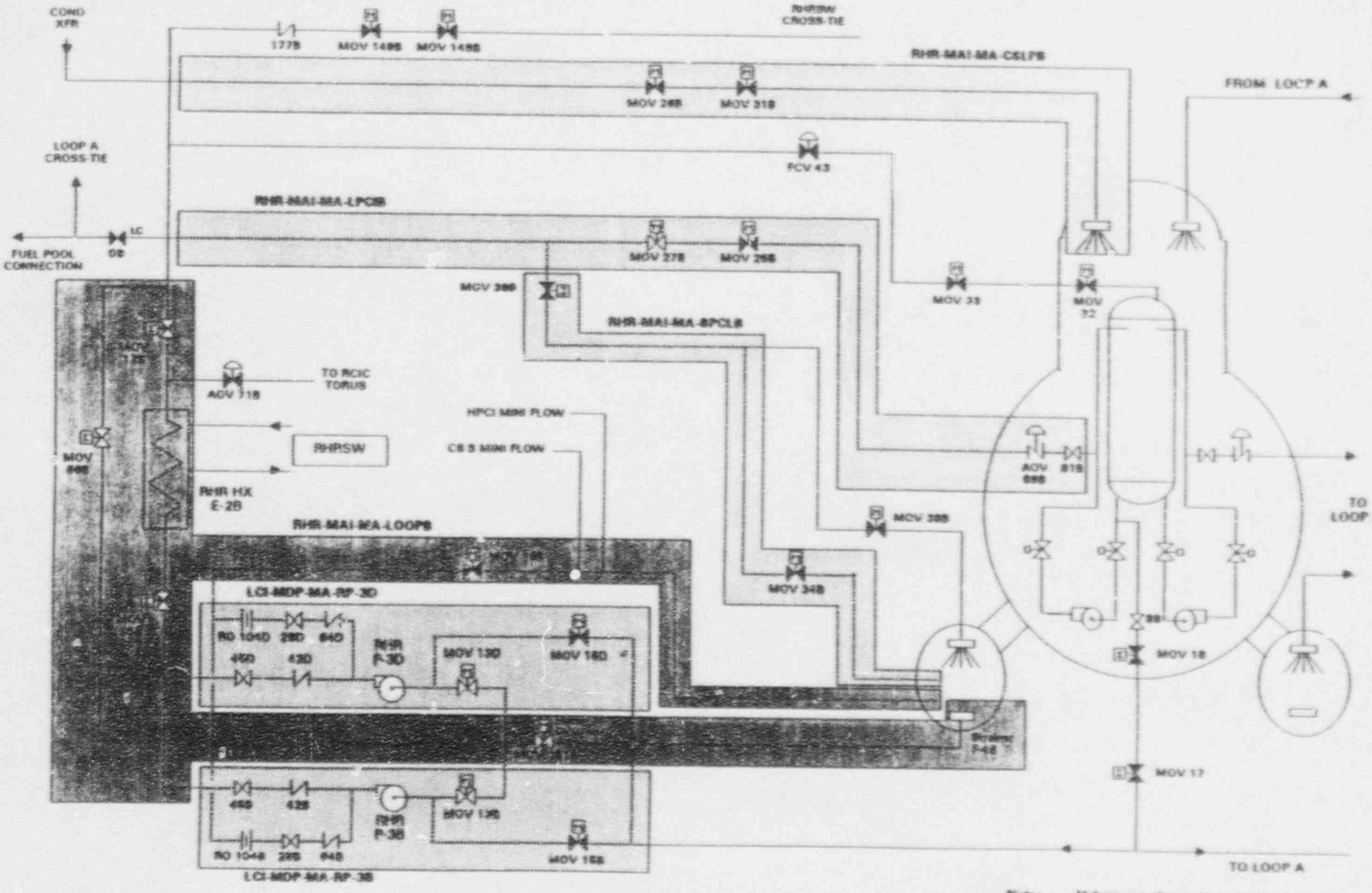


Figure 8.2 RHR System Loop B Component Maintenance Unavailability Allocation

Note: Valves are shown in their standby position.

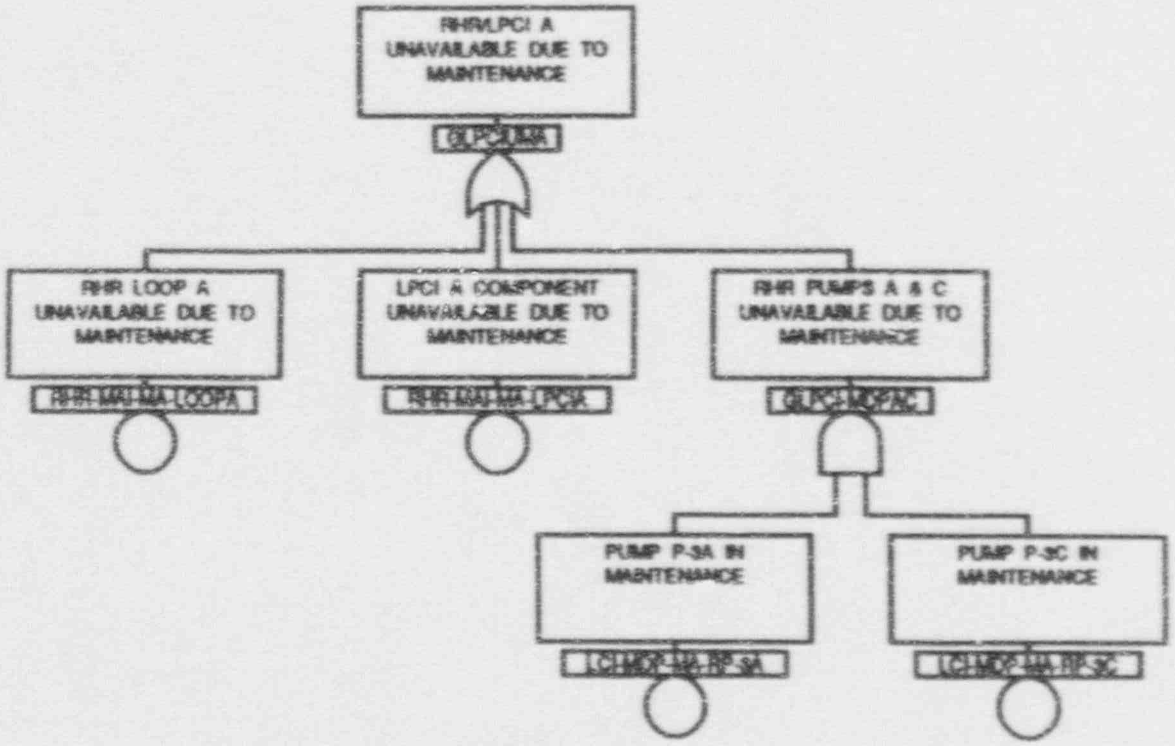

RHR/LPCI A UNAVAILABLE DUE TO MAINTENANCE
GLPCIUMA
RHR LOOP A UNAVAILABLE DUE TO MAINTENANCE
RHR-MAI-MA-LOOPA
LPCI A COMPONENT UNAVAILABLE DUE TO MAINTENANCE
RHR-MAI-MA-LPCIA
RHR PUMPS A & C UNAVAILABLE DUE TO MAINTENANCE
GLPCI-MDPAC
PUMP P-3A IN MAINTENANCE
LCI-MDP-MA-RP-3A
PUMP P-3C IN MAINTENANCE
LCI-MDP-MA-RP-3C

Figure 8.3 RHR/LPCI A Maintenance Unavailability

Item 9

Request

Provide a concise discussion of the treatment of mechanical failure and the overall electrical failure of the Reactor Protection System (RPS) and basis for the probabilistic estimates including derivations used and applicability.

Response

A fault tree model of the RPS and its supporting systems was constructed and quantified. This model addressed mechanical and electrical, random and common-cause failures. Random mechanical faults modeled included a failure to scram because of the scram discharge volume filling with water; common-cause mechanical failures included the failure of two or more adjacent rods to insert and failure of multiple scram discharge valves. Because of the redundancy of mechanical components within the RPS, the contribution of random mechanical failures to the total RPS failure probability is a factor of 10^{-4} less than that of the common-cause mechanical failures. The probability of mechanical failure of the RPS was calculated to be 7×10^{-6}.

Electrical faults modeled included transmitter, relay, and pilot valve solenoid failures in both the RPS and the backup alternate rod insertion (ARI) system. These electrical faults had a combined probability of 2.7×10^{-6}.

In contrast, values of 10^{-5} and 2×10^{-5} were assumed in NUREG/CR-4550 for failures to scram because of mechanical and electrical faults, respectively, at Peach Bottom. While the former value is essentially the same as that calculated for JAF, the latter value is significantly higher. The higher probability of RPS failure because of electrical faults at Peach Bottom results from Peach Bottom not having an alternate rod insertion (ARI) system at the time of the study. In the JAF IPE, a total RPS failure probability of 10^{-5} was assumed. This value is slightly more conservative than that calculated using the fault tree models and is higher than the value of 4.6×10^{-6} reported in the "BWR Owner's Group Response to NRC Generic Letter 83-28, Item 4.5.3", NEDG-30844A, March 1988.

Item 10

Request

Discuss the process used to treat unavailability of the coolant injection function through the Control Rod Drive system to the reactor and the basis for the probabilistic estimates.

Response

The control rod drive (CRD) system provides reactor coolant injection subsequent to the occurrence of a LOCA or transient:

- As an alternative to the core spray and LPCI systems and the RHRSW cross-tie in transients with stuck-open safety-relief valve events and intermediate LOCAs.

- During containment venting if venting is required for containment pressure control.

To inject reactor coolant during containment venting, it was assumed that no enhancement of CRD system flow is required because venting occurs at a late stage in the accident sequence (after 10 hours) by which time lower make-up flows match the reactor decay heat. In particular:

- One control rod drive (CRD) pump operating at a system flow rate of 60 gpm will maintain adequate reactor water level (2/3 core level) in large and intermediate LOCAs, once the reactor power falls--provided that core make-up systems had previously operated for 10 hours.

- For transient scenarios in which continued reactor make-up is required, one control rod drive (CRD) system pump operating at 60 gpm suffices to provide reactor make-up after 8 hours have elapsed.

The unavailability of the CRD system to provide coolant injection during containment venting is occasioned by hardware failures and operator errors in failing to restore manual valve 3CRD-176B to its normally-open position following maintenance of pump 3P-16B and failing to initiate the standby CRD system pump 3P-16B for operation if needed. The CRD was modeled using a fault tree that represents the normal operating configuration, with CRD pump 3P-16A, suction filter 3F-2A and discharge filter 3F-17A in service, and flow control valve 3FCV-19A modulating CRD system flow. Six causes were identified for the CRD system fault tree top event, "CRD Fails to Provide Adequate Flow To Reactor":

- Insufficient water supply to the suction of the CRD system pumps

- Train A suction path hardware failures
- Train A and B strainer failures
- Insufficient flow from CRD systems
- Insufficient flow from pump discharge path
- Insufficient flow from injection path.

These causes contribute to CRD system unavailability. Quantification of the fault tree model led to an unavailability of the CRD system of 7.56 x 10^{-4} (JAF IPE, Volume 1, Table 3.3.6.1).

The CRD system can also be used in a post-accident recovery action as an alternative to the core spray and LPCI systems and the RHRSW cross-tie in large and intermediate LOCAs and stuck-open safety relief valve events. In such a role, human error is expected to dominate the causes of CRD system unavailability though if loss of offsite power has occurred, the loss of instrument air would preclude the use of the CRD system.

Stuck-open SRVs or a LOCA cause a decrease in reactor pressure and an increased rate of reactor coolant inventory loss. If condensate is used to provide reactor make-up, it will eventually fail on inventory depletion. If HPCI is used, it will trip on low reactor pressure at 85 psia. In these circumstances, EOP-2 directs the operators to use the core spray, LPCI or CRD systems to provide coolant make-up. Successful use of the CRD system will, however, require the enhancement of CRD flow by fully opening flow control valves 3FCV-19A/B by manual action from the control room.

The HEP for failing to increase CRD flow is equal to the sum of the probability of failing to determine the need for CRD coolant make-up and the probability of failing to perform the action and then correct the error. Both probabilities were estimated in the IPE as follows:

<u>Operator Fails to Determine Need for Increased CRD Flow</u>.

EOP-2 is being implemented and the operators are instructed to maintain the water level within the reactor pressure vessel. The EOP explicitly lists the systems, of which CRD is one, that can be used as coolant injection sources. The EOP does not, however, instruct the operators to increase CRD flow--they must make this determination.

The time available to the operators to decide to increase CRD flow varies according to the specific accident scenario:

- With an intermediate-size LOCA, the condensate system can provide coolant make-up for approximately 40 minutes before depleting the condenser hotwell inventory. Alternatively, HPCI can provide coolant make-up for approximately 47 minutes before it trips on low reactor steam pressure. Upon the failure of the condensate or HPCI systems, more than 30 minutes remain to increase CRD flow and reestablish coolant injection.

- With three stuck-open safety relief valves (SORVs), the condensate system can provide coolant make-up for approximately 200 minutes before depleting the condenser hotwell inventory. At this time, more than 60 minutes remain to increase CRD flow and reestablish coolant injection.

- With two SORVs, the condensate system can provide coolant make-up for approximately 255 minutes before depleting the condenser hotwell inventory. Alternatively, HPCI can provide coolant make-up for approximately 47 minutes before it trips on low reactor steam pressure. Upon the failure of the condensate or HPCI systems, more than 60 or 30 minutes, respectively, remain to increase CRD flow and reestablish coolant injection.

- With one SORV, the HPCI system can provide coolant make-up for approximately 110 minutes before it trips on low reactor steam pressure. Alternatively, RCIC can provide coolant make-up for approximately 230 minutes before tripping on low steam pressure. Upon the failure of the HPCI of RCIC systems, more than 60 minutes remain to increase and reestablish coolant injection.

Accordingly, values of 10^{-3} and 10^{-4} were assigned to the probability of failing to determine in 30 and 60 minutes, respectively, the need for increasing flow. These probabilities are median values with mean values of 1.6×10^{-3} and 1.6×10^{-4}, respectively, and error factors of 5.

RO Fails to Increase CRD Flow.

Once the operators have determined the need for increased CRD flow, the SS will direct the RO to perform this task. This task is performed in the control room at the 09-5 panel. This task is very straightforward--the RO ensures that the CRD flow control valve 19A/B is fully open by using a control panel switch--and is assumed to be step-by-step with the operator under moderately-high stress.

Accordingly, a value of 0.02 was provisionally assigned to the probability of failing to increase CRD flow. This probability is a median value with a mean value of 0.032 and error factor of 5. The probability was then reduced by a factor of 10 because of the simplicity of this task.

SS Fails to Check RO and Ensure Increased CRD Flow.

Once the SS has instructed the RO to increase CRD flow, the SS will expect confirmation from the RO that the task has been performed. Should this confirmation not be received, the SS will ask for verification. Once the SS has made this request, it is assumed that if the task has not already been performed, the SS will ensure that it will be.

The task of SS checking and correcting the RO is assumed to be step-by-step with the SS under moderately-high stress. Accordingly, a value of 0.2 was assigned to the probability of the SS failing to check and correct the situation. This probability is a median value with mean value of 0.32 and error factor of 5.

Additional details of the derivation of human error probabilities are provided in the JAF IPE, Volume 2, Appendix 2, Section E2.3.4.

Item 11

Request

Discuss the process used to examine the nitrogen ventilation and purge valves as part of sequence development in addition to any individual systems analysis.

Response

Operation of the nitrogen ventilation and purge system was considered only for loss of containment heat removal (TW) sequences in which containment venting is initiated. These are long-term sequences. Venting of the containment is accomplished using AOP-35 "Post Accident Venting of the Primary Containment" which instructs the operator to vent regardless of the radiological consequences. This procedure is entered from EOP-4 "Primary Containment Control" before containment pressure exceeds 44 psig. Sequence development required containment venting if all modes of RHR operation fail. Once the containment vent valves are opened, decay heat removal is achieved by boiling at the suppression pool surface. A description of the nitrogen ventilation and purge system analysis is provided in the JAF IPE, Volume 1, Section 3.2.2.27.

An insight gained in the IPE was that, in the event of loss of all RHRSW pumps, the diesel-driven fire water pump can be aligned to the discharge of RHRSW header A to remove decay heat from the RHR heat exchanger (JAF IPE, Volume 1, Section 1.4.4).

Item 12

Request

Section 3.3.2.2 of the IPE acknowledges that the exposure time for various operating and standby components, and demand spectra (assigned cumulative number of demands for components) for standby components have been estimated for FitzPatrick. Briefly describe the calculations made in estimating these two parameters in the Service Water system and the HPCI system.

Response

The exposure times for various operating and standby components were estimated using data from the plant operating logs, operating procedures, and surveillance test procedures.

The service water system (SWS) normally operates at all times including during plant outages. Accordingly, few demand-related basic events were included in the SWS model other than the failure of non-operating redundant motor-driven pumps to start, the failure of air-operated and check valves to open, and the failure of solenoid valves to energize. The demand failure probabilities for SWS components were based on generic failure data. The operating hours for SWS pumps were approximated by the calendar hours and then used as the exposure hours in calculations of time-related SWS failure rates (e.g., the failure of a pump to continue running). Plant-specific failure rates were then determined by combining plant data with generic failure data in the Bayesian update process described in the JAF IPE, Volume 1, Section 3.3.2.2.

For a standby system (such as the HPCI system), component exposure hours and demand spectra were estimated from detailed reviews of the shift supervisor and nuclear control operator logs, operating procedures and surveillance test procedures. These logs and procedures were used to develop detailed accounts of the performance of each surveillance test and operating procedure. The resulting procedure performance records and their summaries are shown in Tables D.3, D.4, D.6 and D.7 in the JAF IPE, Volume 2, Appendix D. Component level demand matrices were then developed for each procedure (Tables D.5 and D.8), demand spectra for each component were estimated from the procedure performance summaries and its demand matrix, and demand spectra for a given component type were developed by summing all demands for components of that type. The methods used are described in the JAF IPE, Volume 2, Appendix B.

The exposure times used in calculating the probability of the HPCI pumps failing to run were estimated from test data assuming a pump operation test duration of 15 minutes. This duration was based on discussions with plant operators and maintenance staff.

The overall exposure time in tests was calculated as the product of the assumed test duration and the number of tests actually performed. The cumulative hours the pumps were operated in non-test conditions were extracted from plant logs and DSRs. The total exposure time for the HPCI pumps was then obtained by summing the hours for both test and actual operation of the pumps.

Item 13

Request

Describe the process used to treat the following: (A) Common cause failure (fail-to-start mode) of two pumps, (B) Common cause failure (fail-to-continue-to-run mode) of two pumps, (C) Common cause failure (fail-to-open on demand) of two MOVs, (D) Common cause failure of two LPCI batteries to supply power to their loads. Also, describe the treatment of plant-specific common cause factor estimates for two and three stuck-open failure mode of the SRVs.

Response

A common-cause failure is a simultaneous failure of equipment resulting from a shared cause. Industry experience shows that common-cause failures are rare; none were experienced at JAF prior to October 1986--a detailed review of plant information sources such as LERs, operator logs, maintenance work orders, and scram reports revealed no significant events that can be categorized as common-cause failures.

The basic methodology employed in the common-cause failure analysis was that described in NUREG/CR-4550, Volume 1, Revision 1, Section 6 and is described in the JAF IPE, Volume 1, Section 3.2.3.3. To account for potential common-cause failures, redundant components were systematically examined and potential common-cause failures were included in the system models at appropriate levels. Because no JAF plant-specific common-cause failure data were identified, beta factors from NUREG/CR-4550, Volume 1, Revision 1, Table 6.2-1 were used in the development of all common-cause failure probabilities except those for battery failures:

- The beta factors for the common-cause failure of two pumps (fail-to-start mode) were taken from Table 6.2.1 of the NUREG/CR-4550, Volume 1, Revision 1. The beta factor of 0.026 for ESW pumps and RHR service water pumps is the beta factor used for service water motor-driven pumps in NUREG/CR-4550. The beta factor of 0.15 for RHR and core spray pumps is the beta factor for low pressure coolant injection motor-driven pumps.

- The beta factors for the common-cause failure of two pumps (fail-to-continue-to-run mode) were based on the beta factors for similar pumps in the failure-to-start mode. These beta factors were taken from Table 6.2.1 of NUREG/CR-4550, Volume 1, Revision 1, for CWS, ESW, RBC, SWS, TBCLCS, condensate, condensate booster and CRD pumps. The use of the beta factor for the failure-to-start mode in the fail-to-continue-to-run mode is expected to be conservative.

- Common-causes of the failure of two MOVs to open on demand were modeled in the JAF IPE for the following valves:

CSS-CCF-VF-2MOVS	RHR containment spray injection valves
LCI-CCF-VF-2MOVS	LPCI injection valves
LCS-CCF-VF-IMOVS	Core spray injection valves
RSW-CCF-VF-2MOVS	RHR service water valves (for discharge side of RHR heat exchangers)
RSW-CCF-VF-2IJVS	RHR service water valves (for cross-tie)
SPC-CCF-VF-2MOVS	Suppression pool cooling valves
ESW-CCF-CC-101AB	ESW-MOV-101 A and B
RBC-CCF-CC-175AB	RBC-MOV-175 A and B.

  The beta factor of 0.088 is the beta factor for two MOVs failing to operate presented in Table 6.2-1 of NUREG/CR-4550, Volume 1, Revision 1.

- The beta factor of 0.02 for the common-cause failure of two LPCI batteries to supply power to their loads was determined for the JAF dc power system configuration using Table 6 of the dc power study "A Probabilistic Safety Analysis of DC Power Requirements for Nuclear Power Plants," NUREG-0666, 1981.

The estimates of common-cause factors for two and three stuck-open SRVs were based on data for Peach Bottom (Table 4.9-1 of NUREG/CR-4550, Volume 4, Revision 1, Part 1). In 1981 and 1982, two-stage SRVs replaced three-stage SRVs at JAF. Because of their simpler design, two-stage SRVs are much less prone to inadvertent opening than are three-stage SRVs. However, the common-cause failure data used in the JAF IPE are based on the three-stage SRVs installed at Peach Bottom. Two and three stuck-open SRVs were explicitly modeled in the various event trees.

Item 14

Request

Provide a discussion of the treatment of pressure locking of motor operated double disc gate valves and flexible wedge gate valves (experienced at Fitzpatrick in 1988 and 1991, respectively), and impact of corrective actions taken upon the IPE results.

Response

The pressure locking of motor-operated double disc gate valves and flexible wedge gate valves is described in LER-88-013-00, LER-91-006-00/LER-91-006-01, and LER-91-014-00.

The event described in LER-88-013-00 occurred during an outage as part of the post-installation testing of a newly replaced valve and was caused by misinterpretation of valve specifications by the valve manufacturer. Accordingly, this specific event is not relevant to the accident scenarios investigated in the IPE. This notwithstanding, the possible common-cause failure of valves 10-MOV-26A/B was addressed in the fault tree models for JAF.

The events described in the other LERs are failures that would be incorporated in the updated failure rate database to be created as part of the "living PRA" process While the common-cause failure to open on demand of two valves used in the RHR/LPCI and core spray modes of operation and the common-cause miscalibration of reactor pressure transmitters 2-3PT-52A/B/C/D such that all four valves used in the RHR/LPCI and core spray modes of operation fail to open were included in the fault trees developed for the JAF IPE, the possible common-cause failure of all four injection valves to open on demand because of the failure mechanisms described in these LERs was not considered. Accordingly, this possibility too would be introduced into the fault tree models in the living PRA program.

Item 15

Request

Generic letter 88-20 requires licensees to certify that their IPE reflects current plant design and operation. It is our understanding that the operational data provided in Appendix D has been utilized to determine plant specific hardware failure rates only and for the limited period of 1980 to 1986. Since 1986, many changes have occurred, such as design changes, parts supplier changes, manufacturing specification changes, equipment aging, etc., as well as changes in plant personnel training and the plant maintenance programs. This generates a question of whether the Fitzpatrick IPE addresses the current plant status. Please provide a discussion of the impact of plant changes that have occurred since 1986 and the effect of failure rate estimates for the more current period. (Use references as appropriate)

Response

Changes to plant design and operation are described in the modification packages, safety evaluation reports, and operating procedures. The JAF IPE reflected all modifications and operating procedures implemented prior to December 1990. These changes include several that enhance the operability and availability of systems and equipment: the ADS pneumatic supply system upgrade; the RHR suction valve interlock modification; the standby liquid control system solution enrichment for ATWS modification; the installation of the ARI system; the crescent area cooling system modification; the use of firewater injection described in RHR system operating procedure OP-13; LPCI initiation verification; the development of AOP-35 for post-accident venting of the primary containment, AOP-37 for boron injection using the CRD system, AOP-38 for EOP isolation/interlock overrides, and AOP-49 for station blackout; the implementation of the BWR Owner's Group EPG revision 4; and the modification of surveillance test procedure ST-3J to ensure that one core spray train remains operable during the core spray initiation logic function test.

The impact on system reliability and availability of these changes and of changes in operator training and the plant maintenance program should be reflected in the frequency of scrams (i.e., initiating events) and equipment failure rate and unavailability data. All scrams that occurred between January 1976 and December 1989 were included in the initiating event data base used in the IPE--there were no statistical grounds for excluding any data (JAF IPE, Volume 1, Section 3.3.1.1). Therefore, it is only the component failure and unavailability database that can reasonably be regarded as not being fully reflective of current (1992) plant status.

The plant-specific hardware failure and unavailability data were taken from the 6 years of plant operation between 8/11/1980 and 9/30/1986. The data therefore represent plant conditions at the time sequence evaluation and systems analysis began (11/1986). While we would assert this was an entirely reasonable approach, we acknowledge the desirability of maintaining an updated component failure and unavailability database and of using these updated data in the IPE. Accordingly, the Authority will do this in its "living PRA" program.

New plant data are not expected to have a great effect on the component failure data employed within the IPE; nor are they expected to dramatically affect the predicted core damage frequencies. The effect of new plant data will be limited because, as in all recent PRAs, the failure data used in the JAF IPE are an aggregation of plant failure data and generic data (JAF IPE, Volume 1, Section 3.3.2.2). This approach to the development of a plant-specific failure data base is adopted to provide a quantitatively consistent representation of expected equipment performance. With it, the use of generic data and the increased time span for plant data will dampen the effects of any short term change in failure rates.

New plant data may, however, change component and system unavailabilities significantly if tests and maintenance are performed more frequently, because the resulting test and maintenance unavailabilities are not subjected to a Bayesian update process prior to being used in system models.

This notwithstanding, the impact of changes to the predicted core damage frequency that might be occasioned by changes in equipment failure rates and unavailabilities has also been shown to be limited. Sensitivity studies examining the effect of increased system unavailabilities have been performed and submitted to the NRC[4]. The studies concluded that only large increases in the unavailability of the emergency service water (ESW) system would serve to dramatically increase the predicted core damage frequency: while a doubling of the unavailability of the ESW system will result in a 115 percent increase in the predicted core damage frequency, the doubling of the unavailability of other systems will result in increases in predicted core damage frequencies of less than 30 percent.

[4] NYPA letter, R.E. Beedle to T.E. Murley, dated May 28, 1992, respondino to a request for a review of the Fitzpatrick IPE with respect to the NRC's Diagnostic Evaluation Team (DET) Report

Item 16

Request

Fitzpatrick has a wealth of opeiating experience from whicn to update and improve generic human reliability estimates (which would otherwise reed to be utilized in the IPE). Please discuss the process used to capitalize on this experience, specifically with regard to the generation of human error probabilities (HEPs) and perception of human error in the overall results.

Response

Initiating Event Data.

The initiating event frequencies used in the JAF IPE reflect all scrams that occurred between January 1976 and December 1989. Accordingly, human errors that gave rise to scrams are included in plant-specific initiating event frequency calculations reported in the IPE.

Human Error in Pre-Accident Actions.

Historical information for human errors in pre-accident actions were utilized in the JAF-IPE. Scram reports and licensee event reports (LERs) were reviewed to identify incidents to which human errors contributed. The fault trees were then reviewed to ensure that the human errors involved were addressed within the appropr ate system fault trees. No attempt was made, however, to create a JAF plant-specific human error database utilizing these events. Instead, the ASEP-HRAP methodology was used with the additional conservatism that where dependencies could exist in test and maintenance errors, complete dependence was assumed. In assigning probabilities, several mitigating factors were considered:

- Recovery from human errors prior to accident occurrence is often possible given control room indications of valve position and the verification of component status that is performed each shift.

- Flow tests performed as part of post-maintenance testing and the formal verification of equipment status by a second p[illegible]on will significantly reduce the probability of failures to restore components to their proper configuration.

- The common-cause failure of instrumentation is made less likely by an instrument test schedule that staggers instrument tests and ensures that the same work crew is not responsible for all tests on a given set of instruments.

Human Error in Post-Accident Response and Recovery Actions.

The human error probabilicies (HEPs) employed in the JAF IPE were individually determined for each operator action. While the HEPs were based on predictions of the ASEP-HRAP methodology, the values determined were modified to take into account especially clear accident conditions and operator familiarity with them, operator simulator exercises, and the time available to decide upon a particular action and respond to it. Some examples of where ASEP-HRAP predictions were modified in response actions (actions that operators perform in response to plant conditions and are generally demanded by the EOPs) follow. In reviewing these examples, it should be noted that, subsequent to the post-TMI control room design review, significant improvements were made in the labeling and functional demarcation of controls in the control room to eliminate human design deficiencies.

- In an ATWS scenario in which MSIVs are open the probability that the reactor operator fails to initiate standby liquid control(SLC) was provisionally assigned a median value of 0.02 using the ASEP-HRAP methodology. This probability was then reduced by a factor of 10 to account for the immediacy of SLC initiation that is emphasized in JAF training and was substantiated by simulator exercises observed and discussions with the operators. This application of plant experience is described in the JAF IPE Volume 2, Appendix E, Section E2.1.3.2.

- In ATWS scenarios in which MSIVs are open, the probability that the operators fail to diagnose the need to override MSIV isolation is determined in part by the time available to perform the override. To determine this time, measurements were made in simulator exercises. The value for the probability selected from ASEP-HRAP was the lower bound value. The use of this value was justified under ASEP-HRAP guidelines because the accident sequence in question was well practiced and all simulator exercises indicated that operators recognize both the symptoms and need to override MSIV isolation. This application of plant experience is described in the JAF IPE, Volume 2, Appendix E, Section E2.1.4.1.

- In ATWS events with MSIVs closed, a low ($<10^{-5}$) value was assigned to the probability of failing to enter EOPs. This low value was used because of the many indications, alarms and annunciators that notify the operators of entry conditions for the EOPs. It was also observed in simulator exercises that the operators retrieved the EOPs after occurrence of an abnormal event to confirm that EOP entry conditions are met. This application of plant experience is described in the JAF IPE, Volume 2, Appendix E, Section E2.2.1.

- In ATWS events with MSIVs closed, the probability that the operators fail to determine the need for alternate boron injection is determined in part by the time available to make the diagnosis and hence by the time required by the operator to actuate alternative boron injection. This time was measured by following an operator in the simulation of the task in the plant. This application of plant experience is described in the JAF IPE, Appendix E, Sections E2.2.5.1 and E2.2.5.2.

- In ATWS events with MSIVs closed, the probability that the operators fail to provide primary containment control was provisionally assigned a median value of 0.02 using ASEP-HRAP guidelines and tables. This value was then reduced by a factor of 10 because the operators perform this task almost immediately upon a failure to scram, because of the considerable time (approximately 12 hours) available to actuate suppression pool cooling, and because the actuation requires no complex actions and no interface with instrumentation. Similarly, the probability provisionally assigned to the shift supervisor failing to check the operator and correct a failure to implement primary containment control was also reduced by a factor of 10. These applications of plant experience are described in the JAF IPE, Volume 2, Appendix E, Sections E2.2.7.3 and E2.2.7.4.

- In normal transients or LOCAs, a failure to enter the proper EOPs was assigned a low value ($<10^{-5}$) because the operators have memorized the entry conditions for the EOPs and the EOPs are practiced monthly in simulator exercises. Furthermore, as noted above, the operators were observed in simulator exercises to retrieve the EOPs after the occurrence of an abnormal event to check if the entry conditions are met. This application of plant experience is described in the JAF IPE, Volume 2, Appendix E, Section E2.3.1.

- In normal transients or LOCAs, the value assigned from ASEP-HRAP to the probability that the operator fails to defeat HPCI auto-transfer on high torus level is reduced by a factor of 10 because of the relative simplicity of the incident and the time available. This application of plant experience is described in the JAF IPE, Volume 2, Appendix E, Section E2.3.3.2.

- In normal transients or LOCAs, the value assigned using the ASEP-HRAP methodology to the probability that the operator fails to use the CRD for coolant injection was reduced by a factor of 10 because of the simplicity of the task. This application of plant experience is described in the JAF IPE,

- The value assigned using ASEP-HRAP to the probability that the reactor operator fails to depressurize the reactor vessel was reduced by a factor of 10 to account for the simplicity of the task. This application of plant experience is described in the JAF IPE, Volume 2, Appendix E, Section E2.3.5.2. Similarly, the value assigned to the probability that the shift supervisor fails to ensure that the reactor is depressurized was also reduced from the value derived using the ASEP-HRAP methodology. This application of plant experience is described in the JAF IPE, Volume 2, Appendix E, Section E2.3.5.3.

- In normal transients or LOCAs, the calculation of the probability of failing to perform primary containment control relied extensively on plant data. The value for the HEP of the operator failing to vent locally was determined in part by the time required to complete the task. This time was measured in the plant by observing an operator as he simulated the task. Furthermore, the HEP assigned to this task using ASEP-HRAP methodology was reduced by a factor of 10 to account for the emphasis placed on the task in training, the long time available, and the availability of additional personnel to accomplish the task when that needs be done. This application of plant experience is described in the JAF IPE, Volume 2, Appendix E, Section E2.3.6.1.

ASEP-HRAP predictions were also modified for recovery actions. Recovery actions are those that operators perform to recover from specific initiating events or component or system failures that exacerbate the accident. Such actions may include local manual actions. An example of a modification based on plant data and experience follows:

- The probability that operators fail to manually open the core spray or LPCI injection valves as part of recovery actions was determined in part by the time required to manually open valves locally. This time was measured as an operator simulated the actions required at the plant. This application of plant experience is described in the JAF IPE, Volume 2, Appendix E, Section E3.3.1.1.

Item 17

Request

Please identify those instances in which performance shaping factors (PSFs) are used to modify HEPs according to the difficulty of the tasks under analysis, and discuss the rationale for the PSF selection. It appears that the operator response to extremely difficult situations has been evaluated optimistically. For example, for the Anticipated Transient Without Scram (ATWS) initiating event, where the operator has 1 to 3 minutes to recognize that it is an ATWS, the operator must enter EOP-2, follow EOP-2 to the point where he is directed to enter EOP-3, enter EOP-3 and verify that he must initiate Alternate Rod Injections (ARI) and Recirculation Pump Trip (RPT) and override ADS. The IPE, on the basis of Fitzpatrick's good operator training, assumes an HEP less than 1E-5. Describe the PSFs used to account for the stressful situation and the limited time for operator response.

Response

The Authority believes that the operator response was evaluated realistically and not optimistically. This belief is based on numerous interviews and discussions with the reactor operators, training and operations personnel, and observations of operator performance in simulations of several different accident types. The accidents simulated involved many types of failures so that an accurate and realistic evaluation of operator response could be made.

The actions of concern in this discussion are "immediate" emergency actions that must be taken quickly following an abnormal event. While the operators are required to memorize the entry conditions to the EOPs and the operators practice the actions frequently, they are trained to read each step in the procedures prior to performance to ensure that no required action is omitted. Immediate actions are therefore simply operator actions that are among the first steps in the EOPs and thus will be performed expeditiously.

For ATWS events, certain actions can be classified as immediate actions. They include:

- Entering the EOP

- Scramming the reactor (which directly enters the operator into the failure to scram EOP)

- Verifying ARI initiation and RPT

- Overriding ADS.

Verifying ARI and RPT occurrence and overriding ADS were treated as being completely dependent.

The initiating event coupled with a failure to scram will result in the entry conditions for EOP-2 (reactor control) being met. The shift supervisor at JAF does not retrieve this EOP: it is under glass at his station and ready for implementation. The first direction and instruction for EOP-2 addresses whether a scram has occurred and directs a manual scram if it has not. The second decision point addresses whether all rods have been fully inserted. If more than one rod is not fully inserted, entry into EOP-3 is required.

At JAF, there are always at least two reactor operators in the control room: a senior reactor operator who serves as the shift supervisor and a second operator who is required to be at the main control panel (or "horse-shoe") at all times. The reactor operator at the main control panel in the horse-shoe will receive numerous and immediate indications that a failure to scram has occurred:

- A control rod "full-in" light display on panel 9-5 that indicates which control rods are fully inserted

- A computer printout of control rod pocitions.

In addition, there are four shared recorders on the 9-5 panel that can display upto eight IRMs, six APRMs, or a combination of the two, SRM monitors and recorders, ARI controls and indications, RPS group lights, scram valve position indicators, and scram air header pressure indicators.

The EPIC (emergency and plant information computer) monitors also display safety parameters and plant conditions. Three monitors are placed at the shift supervisor station, two at the nuclear control operator's desk, and two above the 9-5 panel. The displays are color-coded and highlight the EOP entry conditions and critical parameters within the EOP.

Given these indications and the fact that a reactor scram is an immediate and much practiced action, a probability of 10^{-3} seems reasonable for a failure to recognize an ATWS (or failure to scram) and then enter EOP-3. A task analysis of the shift supervisor and reactor operator failing to recognize that power is above 2.5 percent and that a failure to scram has occurred further justifies this probability. The events that must occur are as follows:

[1] Reactor operator fails to notice the control rod display and

power indicators (IRMs, APRMs, and SRMs)

[2] Shift supervisor fails to notice the above indications and fails to notice indications on the EPIC display.

[3] Operator fails to recognize that a scram is required (enter EOP-2) and fails to notice that a failure to scram has occurred (enter EOP-3).

Probabilities of 10^{-3}, 10^{-3}, and 10^{-6} were assigned to these steps using Table 8-5 in NUREG/CR-4772.

In performing the IPE, over 20 accident types were observed at the JAF simulator. In every case, regardless of the crew, the operator (shift supervisor) immediately entered the appropriate EOP and correctly performed the immediate actions. Of these simulated accidents, eight were ATWS types.

Item 18

Request

The human reliability analysis (HRA) is based on generic basic human error probabilities (BHEPs) modified by recovery factors (RFs) "which limit undesirable consequences of human error by allowing for human redundancy ..." (pg. 3-379). Thus the HRA reduces the generic BHEP value of 0.03 through the use of RF(s). In the example given on page 3-379 for the calibration of a pressure transmitter, the generic value of 0.03 was used as the HEP for this task for the typical or nominal plant. The generic BHEP is then reduced by a factor of 0.01 to account for post-calibration testing and independent verification. We call your attention to page 5-6 of NUREG/CR-4772 which provides guidance for the use of the methodology you have adopted. Please note that Step 2 on page 5-6 states that "No downward adjustment (of the BHEP) should be made without a more thorough HRA of the kind specified in NUREG/CR-1278". It is our understanding that the BHEP value is assumed to already account for normal or typical "checks & balances" for operator actions. Therefore, the application of RFs to further reduce the BHEP value should be based upon procedures, QA techniques, independent verifications, maintenance practices, etc. which are significantly superior to those typically found in the average or nominal plant. Please take a sample of 5 or 6 nominal human error probabilities (NHEP) values from table 3.3.1 and discuss the RF values used to adjust the BHEP value and discuss how they are supported by factors for FitzPatrick which clearly demonstrate that the Fitzpatrick "checks and balances" are significantly better than those normally utilized in the typical or nominal plant.

Response

The issue raised by this request is whether the application of RFs to the BHEPs for miscalibration and restoration events in the JAF IPE was justified. The reviewers refer to Step 2 on page 5-6 of NUREG/CR-4772 and state that it is their understanding that the BHEP is already assumed to account for normal "checks and balances." This perception, however, represents a misunderstanding of the ASEP HRAP (i.e., NUREG/CR-4772). Step 2 of Table 5-1 (page 5-6 of NUREG/CR-4772) provides guidance on adjusting the BHEP. The statement on page 5-6 that "No downward adjustment should be made without a more thorough HRA..." is not related to the application of RFs but rather to the adjustment of the initial BHEP (for example, to increase the BHEP value of 0.03 if poor human factor conditions exist in the plant). Once the BHEP is selected, the remaining steps in Table 5-1 provide guidance for the application of RFs to the BHEP. The statement in question on page 5-6 is therefore only a caution against downwards adjustments of the BHEP and is unrelated to the application of specific RFs discussed in Step 4 on page 5-7 of NUREG/CR-4772 and in Tables 5-2 and 5-3. This application of specific RFs is a critical and integral part of the ASEP HRAP (NUREG/CR-4772) methodology as is clearly demonstrated in NUREG/CR-4550, Volume 6, and in Dr Swain's comments on the JAF IPE (Item [1]).

Examples of the way in which RFs and other aspects of the ASEP HRAP were applied to adjust the BHEPs for the JAF pre-accident HRA follow. It should be noted that, in his review, Dr Swain concurred with these values and that, in the IPE, the pre-accident HRA was augmented by observations of the instrument functional tests and calibration activities.

Failure to Restore SLC after Test.

Task. Operator tests SLC, opening valves 11SLC-26/27/41. After the test, the operator needs to restore each valve to its proper position.

Activities. This task involves the restoration of the valves to their proper position. Failure to close valves SLC-26/27 will result in a system flow diversion failure when the system on demand. Therefore there are only two activities associated with this task: the closure of valves 11SLC-26/27.

Dependency. Because restoration of the SLC requires that both activities associated with the task be completed successfully, dependence effects are irrelevant and zero dependence is assigned to the activities of this task (see Table 5-1, Item 9.a of NUREG/CR-4772).

Recovery. Independent verification of restoration of valves 11SLC-26/27 is performed by a second person and a written record is made. Accordingly, Optimum Condition #3 (see Table 5-3 in NUREG/CR-4772) applies to both valves. A total recovery factor of 0.1 was taken for each valve (see Table 5-3 in NUREG/CR-4772).

Nominal Human Error Probability. The probability that the operator fails to close a valve is therefore:

$$
\begin{aligned}
NHEP_T &= (BHEP_{SLC-26} * RF) + (BHEP_{SLC-27} * RF) \\
&= (0.03) * (0.1) * 2 \\
&= 6 \times 10^{-3}
\end{aligned}
$$

Miscalibration of ECCS-A ATTS Instrumentation.

Task. Operator calibrates the ECCS a! log tr?nsmitter trip system (ATTS) trip units using procedure ISP-175A. This procedure includes calibrating trip units 02-3-MTU-272A, 02-3-MTU-273A, 02-3-MTU-272C, 02-3-MTU-273C, 02-3-MTU-202A, and 02-3-MTU-202C. The other nine units are not re]evant to the IPE analysis.

Activities. To calibrate ATTS trip units, the operator:

A. Performs a pre-calibration test to determina if the trip unit is calibrated (st-p 5.6.1 in Procedure ISP-175A)

B. Determines the need for calibration by verifying the pre-calibration test (step 5.6.2 in the procedure). If the operator fails to perform this step, it was assumed that the trip unit is out of calibration.

C. Sets the stable current to 12 mA (step 5.6.2.4 of the procedure).

D. Adjusts the meter to obtain a mid-scale setting (step 5.6.2.5 of the procedure).

It was assumed that if the operator successfully performs activity B (i.e., Step 5.6.2), ıen steps 5.6.2.1, 5.6.2.2, and 5.6.2.3 are performed (i.e., it was assumed that once the operator recognizes the need for calibration, he will attempt to do it). Therefore, steps 5.6.2.1, 5.6.2.2, and 5.6.2.3 were not addressed in determining the nom.nal HEP.

Dependency. Because the calibration of a single trip unit requires a series of activities and the failure of any one causes miscalibration, dependence effects are irrelevant and zero dependence is assigned to the activities of this task (see Table 5-1, Item 9.a of NUREG/CR-4772).

Recovery. Step 5.6.2.6 of the procedure requires that the operator verify Step 5.6.1 (i.e., activity A). In essence, the operator performs a post-calibration test. In doing so, the operator is required to write down the results of the verification on a checklist. Optimal conditions #2 and #3 therefore apply (Table 5-2 of NUREG/CR-4772) and a total recovery factor (RF) credit of 0.01 applies (Case VIII, Table 5-3, NUREG/CR-4772).

In addition, a daily check, structured to identify component operability, is performed. Accordingly, Optimal Condition #4 applies and an additional recovery credit can be given, reducing the total recovery factor to 0.001 (Case VII, Table 5-3, NUREG/CR-4772).

Nominal Human Error Probability. The probability that the operator miscalibrates a trip unit is therefore:

$$\begin{aligned} NHEP_{\text{Trip unit}} &= RF * (BHEP_{\text{Activity A}} + BHEP_{\text{Activity B}} + BHEP_{\text{Activity C}} + BHEP_{\text{Activity D}}) \\ &= (0.001) * (0.03 * 4) \\ &= 1.2 \times 10^{-4} \end{aligned}$$

In determining this nominal HEP, it was assumed that if the operator miscalibrates the first unit, he will also miscalibrate subsequent trip units because miscalibration is likely to indicate that the operator does not understand the process. Therefore the probability that the operator miscalibrates all trip units is:

$$NHEP_T = 1.2 \times 10^{-4}$$

Miscalibration of HPCI Steam Line High Flow Transmitters

Task. Operator calibrates the HPCI steam line high flow transmitters using procedures ISP-226A/B. These procedures includes calibrating DPTs 23DPT-76 and 23DPT-77.

Activities. To calibrate pressure transmitters, the operator:

A. Adjusts zero for 0.98 Vdc for 23DPT-76 (step 5.3.3.2 of procedure ISP-226A) and adjust zero for 0.99 Vdc for 23DPT-77 (step 5.4.3.2 of procedure ISP-226B).

B. Adjusts span for 5.01 Vdc for 23DPT-76 (step 5.3.3.3 of procedure ISP-226A) and adjust span for 5.02 Vdc for 23DPT-77 (step 5.4.3.3 of procedure ISP-226B).

Because technical specifications require that the instruments be calibrated regardless of whether calibration is required, pre-calibration tests and their verification are not applicable and were not considered in the HEP evaluation.

Dependency. Because the calibration of a single DPT requires a series of activities and the failure of any one causes miscalibration, dependence effects are irrelevant and zero dependence is assigned to the activities of this task (see Table 5-1, Item 9.a of NUREG/CR-4772).

Recovery. Step 5.3.3.4 of procedures ISP-226A/B requires that the operator verify step 5.3.3.2 (i.e., activities A and B). In essence, therefore, the operator performs a post-calibration test. In doing so, the operator is required to write down the results of the verification on a checklist. Optimal conditions #2 and #3 therefore apply (Table 5-2 of NUREG/CR-4772) and a total recovery factor (RF) credit of 0.01 applies (Case VIII, Table 5-3, NUREG/CR-4772).

In addition, a daily check, structured to identify component operability, is performed. Accordingly, Optimal Condition #4 applies and an additional recovery credit can be given, reducing the total recovery factor to 0.001 (Case VII, Table 5-3, NUREG/CR-4772).

Nominal Human Error Probability. The probability that the operator miscalibrates a pressure transmitter is therefore:

$$NHEP_{DPT} = RF * (BHEP_{Activity\ A} + BHEP_{Activity\ B})$$

$$= (0.001) * (0.03 * 2)$$

$$= 6 \times 10^{-5}$$

In determining this nominal HEP, it was assumed that if the operator miscalibrates the first transmitter, he will also miscalibrate the second transmitter because miscalibration is likely to indicate that the operator does not understand the process. Therefore the probability that the operator miscalibrates both transmitters is:

$$NHEP_T = 6 \times 10^{-5}$$

Miscalibration of HPCI Pump Suction Low Pressure Switch.

Task. Operator calibrates HPCI pump suction switch 23PS-84B using procedure IMP-23.9.

Activities. To calibrate pressure switch 23PS-84B, the operator:

A. Performs a pre-calibration test to determine if the switch is miscalibrated (step 5.2.2.1 of procedure IMP-23.9).

B. Determines the need for calibration by verifying the pre-calibration (step 5.2.2.2 of the procedure). If the operator fails to perform this step, it was assumed that the switch was miscalibrated.

C. Applies a decreasing pressure to trip point and adjust the pressure switch to increase or reduce pressure for 15 in. (step 5.2.3.3).

D. Applies a decreasing pressure to in. (step 5.2.3.4).

E. Increases the applied pressure .nd verify instrument resets (step 5.2.3.5).

F. Increases the applied pressure to 0 in. (step 5.2.3.6).

Dependency. Because the calibration of a single switch requires a series of activities and the failure of any one causes miscalibration, dependence effects are irrelevant and zero dependence is assigned to the activities of this task (see Table 5-1, Item 9.a of NUREG/CR-4772).

Recovery. Step 5.3.3.8 of the procedure requires that the operator verify step 5.2.2.1 (i.e., activity A), In essence, therefore, the operator performs a post-calibration test. In doing so, the operator is required to write down the results of the verification on a checklist. Optimal Conditions #2 and #3 therefore apply (Table 5-2 of NUREG/CR-4772) and a total recovery factor (RF) credit of 0.01 applies (Case VIII, Table 5-3, NUREG/CR-4772).

Nominal Human Error Probability. The probability that the operator miscalibrates a switch is therefore:

$$\begin{aligned} NHEP_{PS} &= RF * (BHEP_{Activity\ A} + BHEP_{Activity\ B} + \\ &\qquad BHEP_{Activity\ C} + BHEP_{Activity\ D} + \\ &\qquad BHEP_{Activity\ E} + BHEP_{Activity\ F}) \\ &= (0.01) * (0.03 * 6) \\ &\sim 1.8 \times 10^{-3} \end{aligned}$$

Miscalibration of Reactor Protection System (RPS) Average Power Range Monitor (APRM) Instrumentation.

Task. Operator calibrates RPS APRMs APRM-A to F using procedure ISP-20-1.

Activities. To calibrate APRM instrumentation, the operator:

A. Performs a pre-calibration test to determine if the APRM instrument is miscalibrated (steps 5.2.2, 5.2.3, 5.2.4, 5.2.5, and 5.2.6 of procedure ISP-20-1).

B. Determines the need for calibration by verifying the pre-calibration (step 5.3 of the procedure). If the operator fails to perform this step, it was assumed that the APRM instrument is out of calibration.

C. Adjust the power test potentiometer (Z36-R2) to the minimum position (step 5.3.1 of procedure).

D. Momentarily short the front panel meter (M1) and mechanically zero the meter (step 5.3.2).

E. Adjust power test potentiometer (Z36-R2) for 10 V and adjust Z31-R26 for a meter indication of 125 percent (step 5.3.3 of procedure).

Dependency. Because the calibration of a single APRM requires a series of activities and the failure of any one causes miscalibration, dependence effects are irrelevant and zero dependence is assigned to the activities of this task (see Table 5-1, Item 9.a of NUREG/CR-4772).

Recovery. Step 5.3.4 of the procedure requires that the operator verify step 5.2.6, In essence, therefore, the operator performs a post-calibration test. In doing so, the operator is required to write down the results of the verification on a checklist. Optimal Conditions #2 and #3 therefore apply (Table 5-2 of NUREG/CR-4772) and a total recovery factor (RF) credit of 0.01 applies (Case VIII, Table 5-3, NUREG/CR-4772).

In addition, a daily check, structured to identify component operability, is performed. Accordingly, Optimal Condition #4 applies and an additional recovery credit can be given, reducing the total recovery factor to 0.001 (Case VII, Table 5-3, NUREG/CR-4772).

Nominal Human Error Probability. The probability that the operator miscalibrates a switch is therefore:

$$\begin{aligned} NHEP_{PS} &= RF * (BHEP_{Activity\ A} + BHEP_{Activity\ B} + \\ &\qquad BHEP_{Activity\ C} + BHEP_{Activity\ D} + \\ &\qquad BHEP_{Activity\ E}) \\ &= (0.001) * (0.03 * 5) \\ &= 1.5 \times 10^{-4} \end{aligned}$$

In determining this nominal HEP, it was assumed that if the operator miscalibrates the first instrument, he will also miscalibrate other instruments because miscalibration is likely to indicate that the operator does not understand the process. Therefore the probability that the operator miscalibrates all instruments is:

$$NHEP_T = 1.5 \times 10^{-4}$$

Item 19

Request

Please describe and discuss your analysis of operational experience (i.e. LERS, training material and procedures updates, maintenance and surveillance test records, etc.) used to identify human error initiated events and common cause failures.

Response

With the exception of initiating events, no attempt was made to integrate plant human error data into a plant-specific human error data base. Instead, an analysis of operating experience was made to identify potential human errors. These errors were then explicitly depicted in the system fault tree models. The analysis of operating experience entailed the review of the LERs, scram reports, shift supervisor and nuclear control operator logs, maintenance work requests, and the training department's system lesson plan. The role of plant experience in generating human error probabilities is described in more detail in the response to Item 16.

As noted in the response to Item 13, no common-cause failures occurred at the plant between August 1980 and September 1986. However, potential common-cause events identified from the review of operating experience were included in the system models. For example the fault trees modeled common-cause failures of four diesels and of two LPCI injection valves, etc.

As noted in Item 16, observations of simulator performance and walkthroughs of response and recovery actions were also used in developing HEPs for post-accident response and recovery actions.

It should also be noted that the reactor operator training program at JAF now includes a lesson plan (NET-238.13) directly related to the JAF IPE. Furthermore, the training program is kept current by addressing potential operator errors and common-cause failures identified in LERs and other reports of operating experience from JAF and other nuclear power plants.

Item 20

Request

Please specify the BHEP and any RFs used to estimate the probability (NHEP) of failure to vent the wetwell (local operation) upon demand (i.e. Containment Pressure ≥44 psig), and discuss the basis for selection of the BHEP and RF values. Relevant factors to be discussed include the EOP covering containment venting, location and operator access to vent valves and/or their controls, training of the operators required to perform the venting function as well as the effect of such factors as stress, time, and environmental conditions such as temperature and radiation levels expected to exist in the locality of the vent valve controls.

Response

Wetwell venting is normally initiated at the primary containment and purge (PCP) panel located in the relay room. For accident sequences in which motive power is unavailable to the valves, the operator would locally hand-wheel the valves open. Venting of the containment is accomplished using AOP-35 "Post Accident Venting of the Primary Containment." This procedure instructs the operator to vent the containment regardless of the radiological consequences. The procedure is entered from EOP-4 "Primary Containment Control" before the containment pressure exceeds 44 psig. The operators are well trained in the implementation of the EOPs. Although it was not possible to simulate a scenario which led to containment venting, because of the long duration of TW sequences, as part of the HRA the operators did walk through the process involved in implementing AOP-35 both from the PCP panel and locally at each valve.

The controls for the wetwell and drywell vent valves are located in the relay room on panel PCP. This area is easily accessible from the control room and is identified as a mild environment for equipment qualification purposes. The wetwell vent valves are located in the reactor building on the 272 ft elevation just outside the reactor building air lock. This area is accessible in all accident scenarios until core damage occurs. No credit was taken for use of the drywell vent valves in containment venting.

The mean HEP for failure to vent containment from the relay room is 2.6×10^{-3} with an error factor of 10. This HEP was calculated as the sum of two terms:

- The probability that the operators fail to determine containment control/venting is needed

- The product of the probability that the reactor operator fails to perform containment control/venting and the probability that the shift supervisor fails to check the reactor operator and correct the failure to implement venting.

The probability that the operators fail to determine containment control/venting is needed was assigned a median value $<10^{-5}$ and an error factor of 10. This probability is based on the ASEP/HRAP procedure (NUREG/CR-4772) and the fact that 8 hours are available to make this diagnosis. A mean probability of 0.0032 was assigned to the reactor operator failing to perform containment control or venting from the relay room. This probability is based on the fact that the task is relatively straightforward, is described step-by-step in AOP-35, and requires no complex actions on the part of the operator. A mean value of 0.5 was assigned to the probability of the shift supervisor failing to check the RO and correct containment control by venting. This probability assumes a dynamic task with the shift supervisor under moderately high stress. The derivation of these HEPs is detailed in the JAF IPE, Volume 2, Appendix E, Section 2.2.7.

The mean HEP for failure to vent containment via local manual valve operation is 3.2×10^{-3} with an error factor of 10. This value was calculated assuming that the operators have already correctly diagnosed the need for containment venting. Local venting is assumed to be a step-by-step task with the operator under moderately high stress. The derivation of this HEP is detailed in the JAF IPE, Volume 2, Appendix E, Section 2.3.6.1.

Item 21

Request

Table 4.5.1.1 indicates an internal containment failure pressure for Peach Bottom (PB) of 150 psig. NUREG-1150 identifies an estimated mean failure pressure of 148 psig for PB. In Section 4.5.1 Static Over Pressure Containment Failure, you use a containment failure pressure of 159 psig for Peach Bottom and reduce it by 12-13% (to account for thinner vent line bellows at Fitzpatrick) to obtain a failure pressure of 140 psig for the Fitzpatrick IPE. Please provide your basis for using the 159 psig value as a basis for determining the estimated failure pressure rather than the 150 psig value from your comparison of Fitzpatrick vs. Peach Bottom Major Plant Features (Table 4.5.1.1) or the 148 psig value from NUREG 1150 (Vol.1, page 4-12). Use of the 148 or 150 psig values would result in an estimate of failure pressure for Fitzpatrick of about 130 psig. Please discuss the effects of this lower value on the timing and probability of overpressure containment failures. In addition, Section 4.6.1-Selection of the CET seems to indicate that, in spite of the above comparison between PB and Fitzpatrick, the PB containment probabilities and failure modes were used in the FitzPatrick CET. Please clarify this statement and discuss the comparison of the two plants and how it has been used to assign values to the Fitzpatrick CET.

Response

The 148 psig internal containment failure pressure for Peach Bottom is that presented in NUREG-1150. The 150-psig value presented in Table 4.5.1.1 was taken from NUREG/CR-4551 and presumably is 148 psig rounded up. The 159 psig containment failure pressure is the ultimate Peach Bottom Unit 2 containment failure pressure predicted in the "Mark I Containment Severe Accident Analysis" performed by Chicago Bridge and Iron (CBI).

In the JAF IPE, the containment failure modes and probabilities derived for Peach Bottom were used. The justification for this is as follows:

- An analysis performed by CBI[5], comparing the containment at JAF with that at Peach Bottom concluded that the "(JAF) containment is generally as strong (as) or stronger than the reference structure." In this analysis, CBI compared the materials of construction used in JAF and Peach Bottom and examined the major structural components in the drywell and wetwell at both plants. The areas examined included the:

[5] CBI Technical Services Co. "Scoping Study of Mark I Containment Vessel," April 1991

- Drywell head region
- Transition knuckle between the cylindrical and hemispherical portions of the containment structure
- Top and bottom cylindrical regions
- Top and bottom halves of the wetwell
- Vent line bellows.

The study found that the top part of the torus shell and vent line bellows at JAF were thinner than at Peach Bottom. As a result, CBI concluded that the thinner torus shell would decrease the containment failure pressure by 2 psi and that the thinner vent line bellows may result in a 12 to 13 percent decrease in the bellows failure pressure compared to Peach Bottom. However, these differences are not expected to influence the ultimate containment failure pressure.

■ Both plants are BWR4s with Mark I containments. Therefore, containment failure characterizations (static overpressure failure, basemat ablation, isolation failures, drywell liner failure by contact with core debris, etc.) are not expected to differ.

Accordingly, the Authority decided that the containment failure probabilities and modes assumed at Peach Bottom were appropriate for use in the JAF CET. This notwithstanding, a 140-psig containment failure pressure was assumed in the JAF IPE, to obtain conservative estimates of the time at which containment failure occurs--a lower containment failure pressure will result in containment failure occurring earlier. However, it must be noted that containment failure will still not occur until many hours after initiation of the accident. (The MARCH code predicts containment failure will occur at 29 hours assuming a containment failure pressure of 132 psia).

A reduced containment failure pressure will also increase the probability of drywell/wetwell overpressure failure and reduce the probability of failures attributable to wetwell venting. Nevertheless, the minor effects on the timing and probability of overpressure containment failures will not materially change the accident progression insights gained or conclusions drawn in Volume 1, Sections 4.7.4 and 7 of the JAF IPE.

Item 22

Request

Please clarify the apparent discrepancy concerning the amount of Zircalloy available. Tables 4.2.2.1 and 4.5.1.1 indicate a Zircalloy core inventory of 111,216 lb. However, Table 4.3.2.2 indicates a total core inventory of 131,051 lb. Which value is correct? Which value was used in the IPE? In the event that the smaller value is incorrect and was used in the IPE, discuss the impact of the larger value.

Response

Both values are correct. The value found in Table 4.2.2.1 (111,216 lb of zircalloy) reflects the load design for fuel cycle 6. The value found in Table 4.5.1.1 (131,051 lb of zircalloy) reflects the original reactor fuel loading and was assumed to represent the maximum amount of zircalloy in any future load cycle. The larger value was used in the IPE to ensure that calculations of hydrogen release were conservative.

Item 23

Request

With regard to Section 4.5.4-Containment Isolation System (CIS) Failures please identify the CIS failure probability(s) used in the IPE, and contributors to CIS failure. Please identify the necessary failures for the three SBO bypass leak paths identified in Section 4.5.4 and provide the basis for your conclusion regarding their improbability.

Response

The only CIS failure probabilities used in the JAF IPE apply to the SBO bypass leak paths. In station blackout sequences with dc power initially unavailable, three lines that penetrate primary containment remain unisolated providing potential leak paths to the environment for gaseous fission products. These leak paths are:

- Through the drywell sump (equipment drain) line to the radwaste system

- From the reactor water cleanup (RWCU) system into the RWCU pump room or RWCU cleanup filter room

- Into the reactor building closed loop cooling system (RBCLCS) from the recirculation pumps.

The failures necessary to establish a containment leakage path and the probabilities of their occurrence are as follows.

Leakage through the drywell sump line requires that the drywell sump pump discharge line outboard isolation valve fail open. The valve is designed to fail closed on loss of instrument air or power. Given that the mean probability of a solenoid valve failing to close on demand is 10^{-3} (NUREG/CR-4550 ASEP) and the core damage frequency occasioned by internal events at JAF is 1.92 x 10^{-6} year, the probability of core damage and this valve failing to close is $<10^{-8}$/year. Accordingly, this leak path was eliminated from further consideration.

The leak paths through the RWCU and RBCLCS require that a breach of the system piping occur for a containment leakage path to exist because the RWCU and RBCLCS are closed systems inside containment. Given the 10^{-9}/hr/100 ft median probability of piping failures used in the JAF IPE, the probability of a leakage path through the three lines is remote. Furthermore, as the resulting leakage paths involve small-size piping (<4 in. diameter), the leaks would be insignificant.

Item 24

Request

With regard to Section 4.5.5-Containment Electrical Penetration Failures, please provide plots of containment atmosphere temperature vs. time from the MAAP-3.0B analysis for accidents with Direct Containment Heating (DCH). Compare the electrical penetration environmental qualification temperatures to the temperature profiles predicted for DCH events from the MAAP runs, and provide your basis for concluding that the probability of electrical penetration failures is so small that they need not be considered as a possible containment failure mode. Please identify and discuss the process used to treat any active or passive equipment located in the drywell which is assumed or required to function during DCH events.

Response

Section 4.5.5 of the JAF IPE states "...electrical penetration failures were not considered to be a possible containment failure mode." While this statement presents the conclusion of the Authority evaluation of electrical penetration failure, it is somewhat misleading in that it gives the impression that electrical penetration failures were dismissed without being modeled. In fact, to conservatively reflect previous treatments (e.g., NUREG-1150), electrical penetration failures caused by extreme thermal environments were modeled in the JAF IPE as drywell failures rather than as separate containment failure modes. The probability of thermal failure of the electrical penetrations is therefore accounted for in the JAF IPE in exactly the same way that it was accounted for in the Peach Bottom Level 2 PRA (NUREG/CR-4551, Volume 4, Revision 1, Part 2, Appendix A)--thermal failure of the electrical penetrations was treated as an additional mode of drywell failure in evaluating the likelihood of containment failure and determining source terms.

Thermal failures of the containment are addressed in the JAF containment event tree (CET). Question 128 of the CET asks "Does the containment fail at low pressure from temperature in the drywell?" Two outcomes for this question are (1) LTCF - "Late Thermal Containment Failure"; and (2) n:LTCF - "no Late Thermal Containment Failure." Three cases define the circumstances under which this question is evaluated. The first case captures all accident sequences in which the containment has not failed prior to or as a consequence of events at vessel breach and thus is still at high pressure (i.e., no venting has occurred). The second case captures all accident sequences in which thermal failure of the electrical penetrations would not be considered, either because there is no thermal load (and hence no thermal failure) or because a drywell failure had previously occurred with any of the following conditions existing:

- There is no vessel failure (i.e., the accident has been arrested in the vessel and no reasonable mode of electrical penetration failure can be cited)

- The containment has failed in the drywell (in which case thermal failure of electrical penetrations is moot)

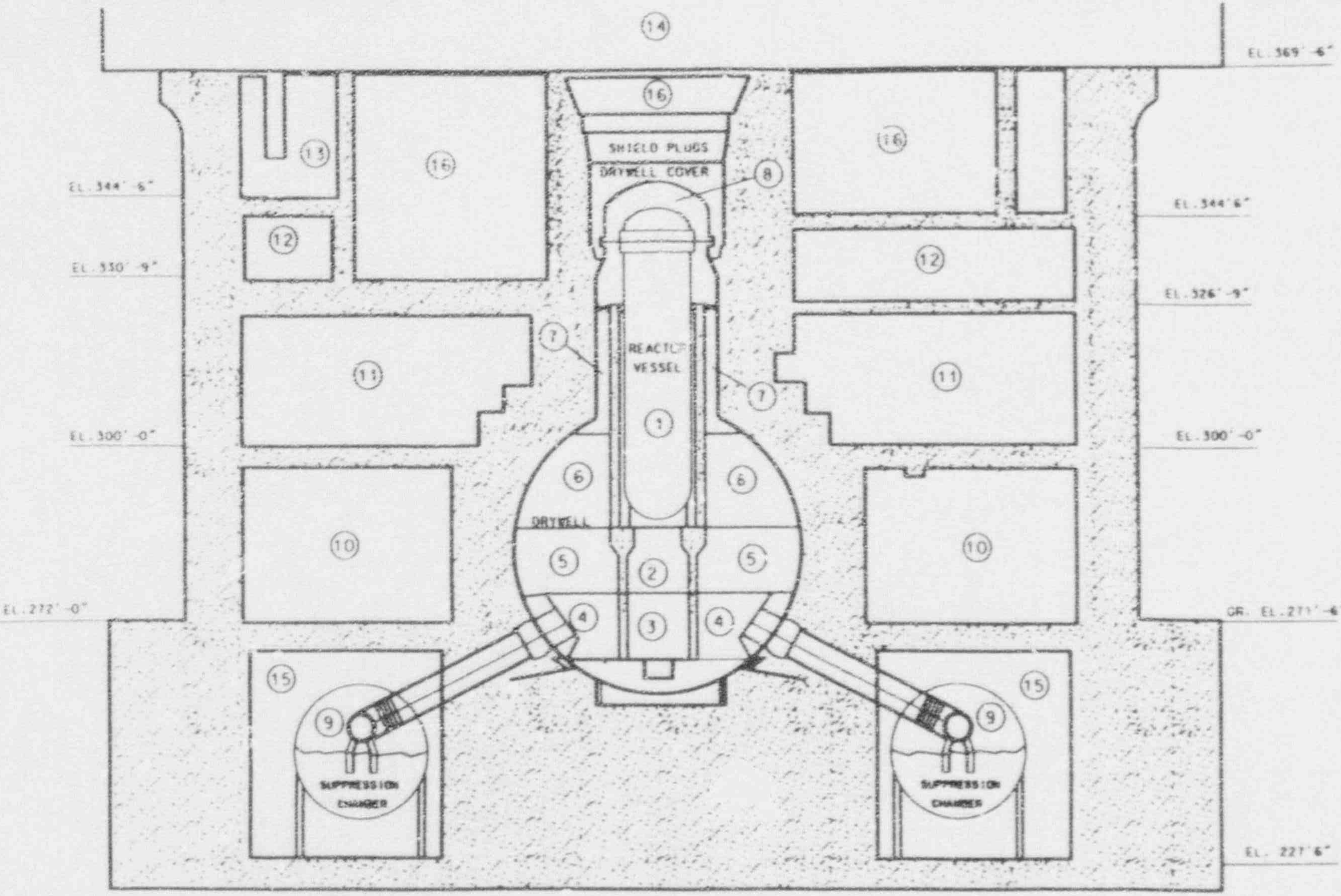
- A deep water pool covers the debris and cools escaping gases (in which case no thermal load would challenge the electrical penetrations).

The third case captures those sequences in which the wetwell has failed and a significant thermal load exists. In this third case, the probability of thermal failure is approximately 25 percent, this probability being the value used for Peach Bottom in NUREG/CR-4551, Volume 4, Revision 1.

The wording of the request for Item 24 indicates that the reviewers believe that MAAP 3.0B calculations were performed to assess containment performance under loads associated with vessel failure. MAAP 3.0B, was not used in the JAF IPE. The principal tool for assessing plant-specific containment loads at JAF, as indicated in Section 4.3.1 of the JAF IPE, was BWRSAR. Calculations performed with this code, supplemented by an evaluation of studies of Mark I containment performance, were used to quantify the IPE back-end model.

Based on BWRSAR calculations, drywell temperature profiles after vessel breach prepared for all five plant damage states (JAF IPE, Volume 2, Appendix I) predict temperatures below the electrical penetration environmental qualification temperatures. The Authority, therefore, concluded that drywell temperatures anticipated during postulated severe accidents should not cause the sealant material to fail. Subsequently, the CONTAIN 1.12 computer code was used to validate this conclusion. Figure 24.1 presents the primary containment nodalization used in the CONTAIN analysis.

The principal challenge to electrical penetrations comes from molten core-concrete interactions that occur in the absence of a significant overlying water pool. Because hot gases sparging through the molten debris will heat the drywell airspace, drywell sprays are the only effective mechanism to cool the air. However, because the core damage frequency for JAF is dominated by non-recovered station blackouts, drywell sprays would not be



NODALIZATION:

CELL 1 - DRYWELL IN-PEDESTAL 1
(283'1" - 350'4.75")

CELL 2 - DRYWELL IN-PEDESTAL 2
(264'7" - 283'1")

CELL 3 - DRYWELL IN-PEDESTAL 3
(252'6" - 264'7")

CELL 4 - DRYWELL EX-PEDESTAL 1
(256'6" - 264'7"+VENTS 243'7")

CELL 5 - DRYWELL EX-PEDESTAL 2
(264'7" - 278'0")

CELL 6 - DRYWELL EX-PEDESTAL 3
(278'0" - 305'6")

CELL 7 - DRYWELL UPPER PART
(305'6" - 355'8.75")

CELL 8 - DRYWELL STEEL HEAD
(345'8.75" - 359')

CELL 9 - WETWELL AIR VOLUME
(243'7" - 259'6")

CELL 10 - REACTOR BUILDING
(272' - 298'6")

CELL 11 - REACTOR BUILDING
(300' - 325'3")

CELL 12 - REACTOR BUILDING
(328'9" - 343')

CELL 13 - REACTOR BUILDING
(344'6" - 363'6")

CELL 14 - REACTOR BUILDING
(ABOVE 367'6")

CELL 15 - OUTER TORUS

CELL 16 - VOLUME ABOVE DRYWELL HEAD
(342'0.375" - 363'5")

CELL 17 - ENVIRONMENT CELL

Figure 24.1 CONTAIN Primary Containment Nodalization

available in most accidents. Therefore, the CONTAIN 1.12 DCH analysis assumes the long-term high pressure accident progression calculated for plant damage state 1 by BWRSAR.

At vessel breach, the sudden vessel depressurization which occurs when the first instrument tube fails results in a rapid rush of hot steam through the hot particle debris bed accumulated in the bottom head of the vessel. This steam immediately reacts with unoxidized zirconium producing large amounts of highly superheated hydrogen (Figure 24.2). Of particular interest is the fact that while the reactor system is depressurizing (Figures 24.2 and 24.3), essentially no steam flows out of the failed instrument tube. To produce a bounding calculation it was assumed that the hydrogen exiting the vessel during depressurization remains at the debris temperature for the entire blowdown--the energy evolved in the metal water reaction was assumed to heat the debris bed and the produced gas was assumed to follow the debris bed temperature. The results of this calculation are shown in Figure 24.4 and 24.5. The pressure rise (Figure 24.4) does not significantly impact containment integrity. Figure 24.5 shows that although the temperature increase in the reactor cavity cells (drywell in-pedestal 2 and 3 location) is significant, the temperature response elsewhere in the drywell is mild. In particular, the drywell temperature profile for drywell ex-pedestal 3, which includes all the electrical penetrations inside the drywell depicts temperatures lower than the electrical penetration environmental qualification temperatures of 340°F to 390°F. Therefore, the CONTAIN 1.12 results reaffirm the original conclusion that electrical penetrations failures are not considered to be a possible containment failure mode.

Among other equipment failures, other than those of electrical penetrations, failure of the reactor pedestal and potential drywell bypass is the principal challenge from direct containment heating (DCH). The JAF IPE accounts for reactor pedestal failure in the same manner as did the Peach Bottom NUREG/CR-4551 analysis because the design is very similar. No other equipment failures are of importance because most of the active equipment in a BWR is outside containment. The notable exceptions to this are the safety/relief valves and parts of the reactor pressure vessel level instrumentation but these items are irrelevant once the reactor vessel is breached.

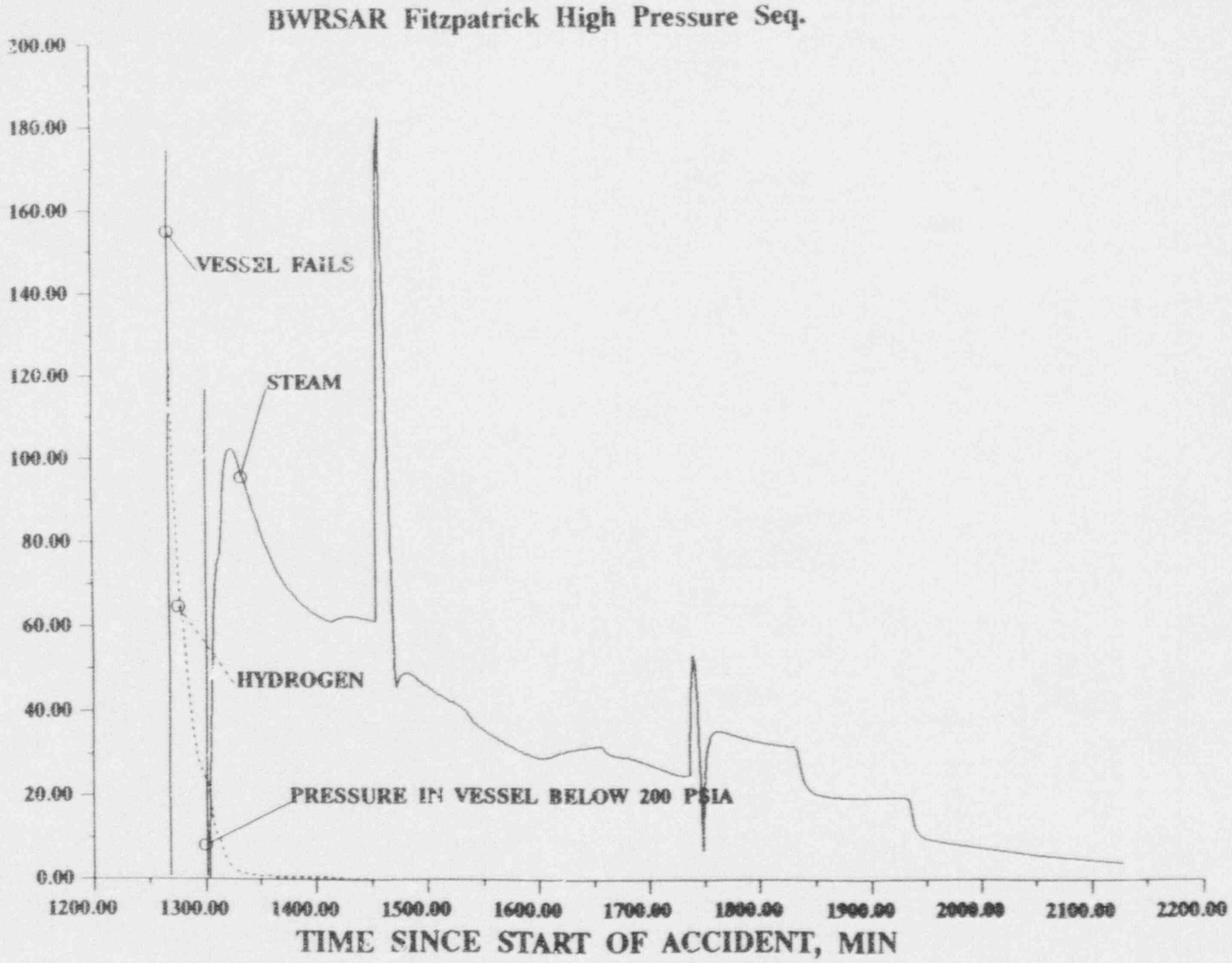


Figure 24.2 BWRSAR Fitzpatrick High Pressure Sequence-Flow out of Vessel

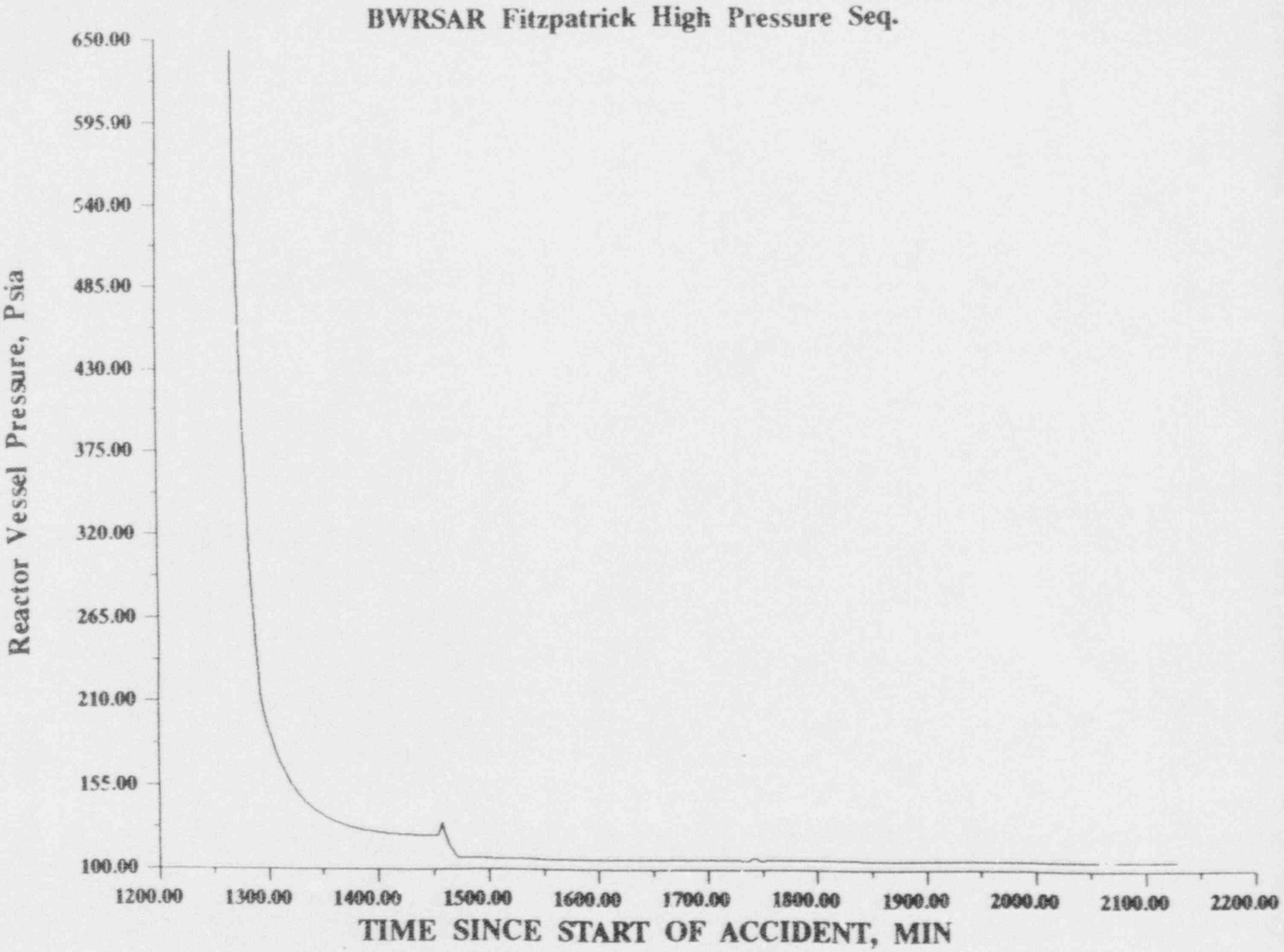


Figure 24.3 BWRSAR Fitzpatrick High Pressure Sequence-Vessel Pressure

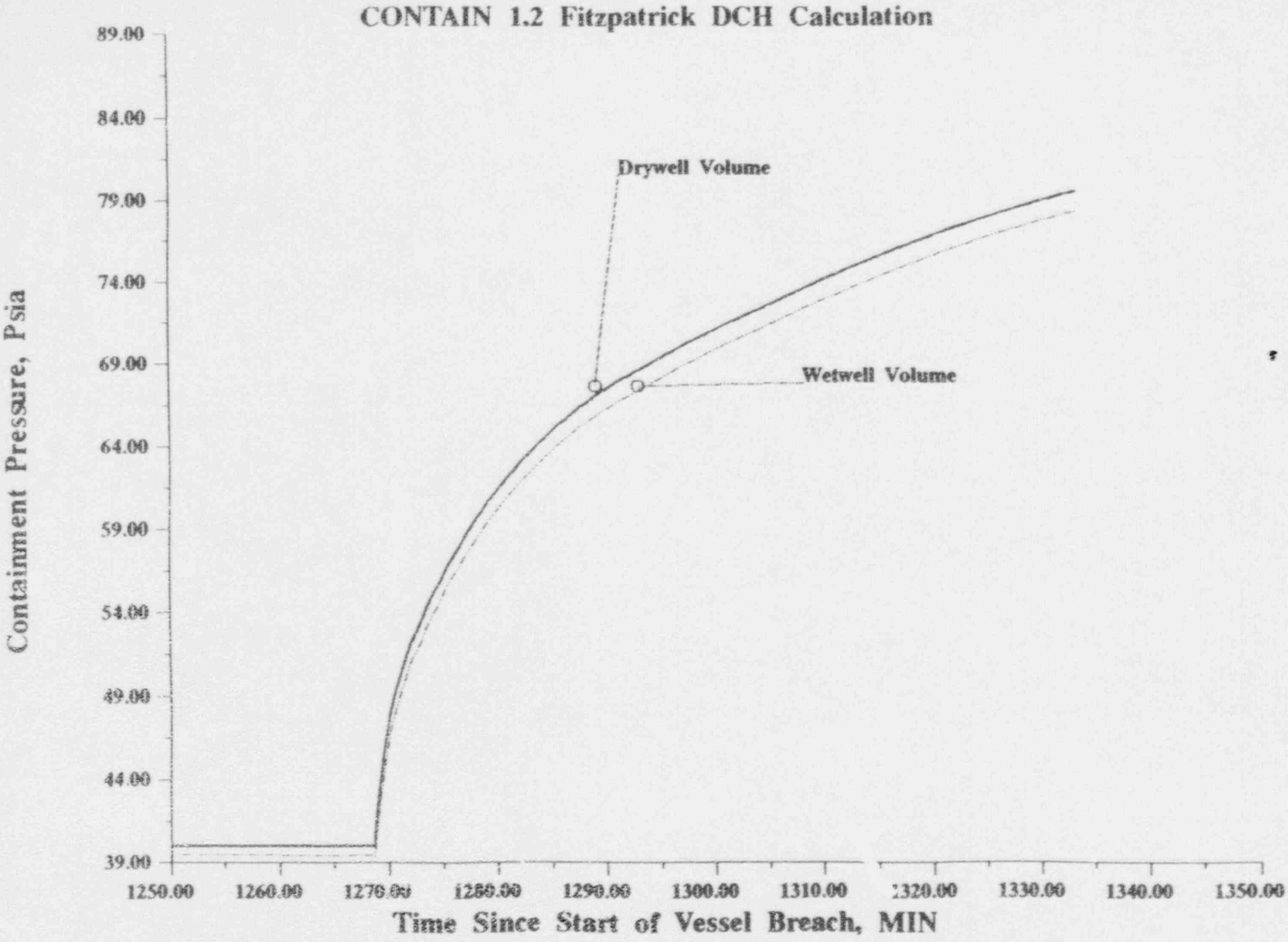


Figure 24.4 CONTAIN Fitzpatrick DCH Calculation-Containment Pressure Profile

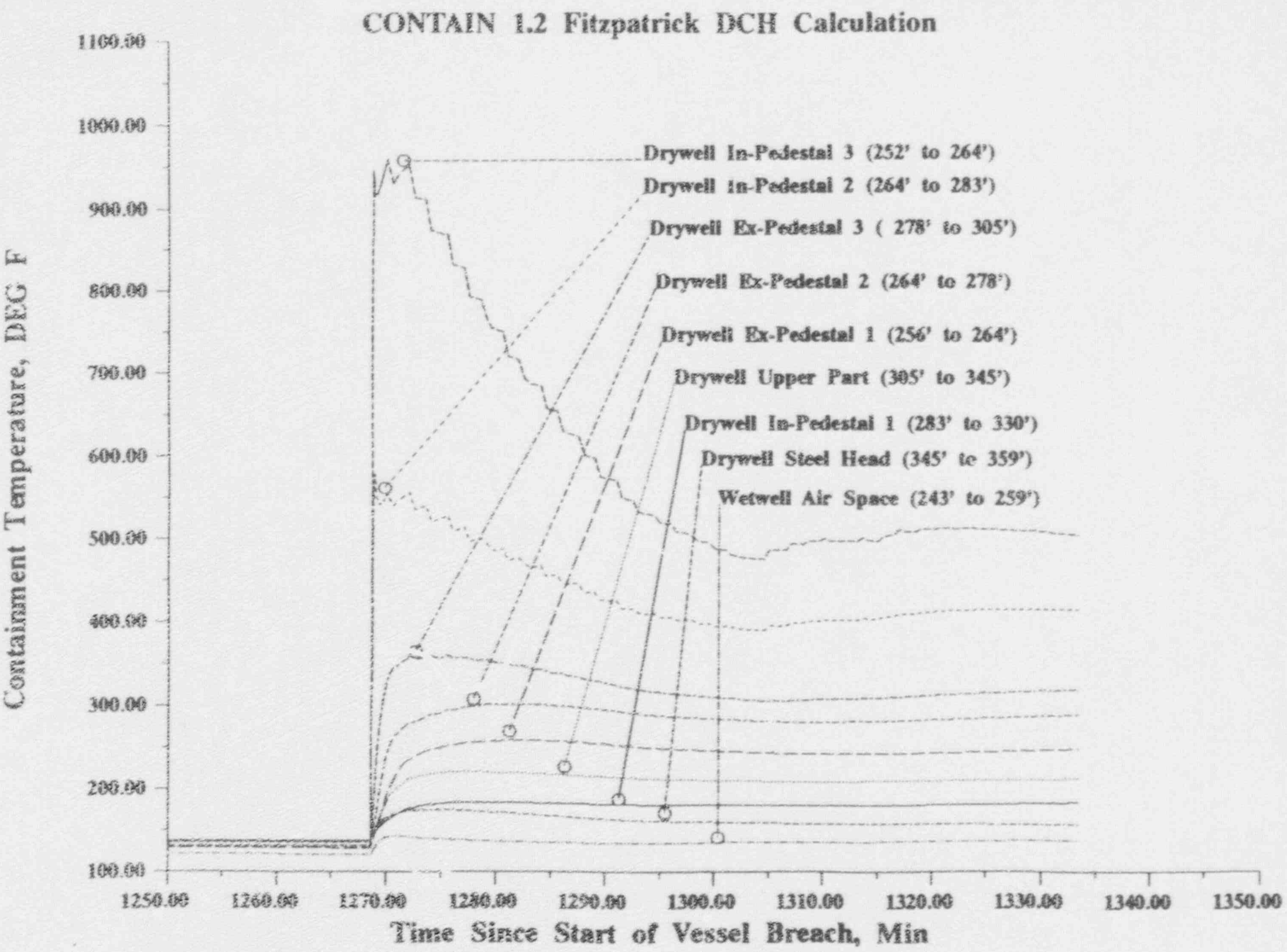


Figure 24.5 CONTAIN Fitzpatrick DCH Calculation-Containment Temperature Profile

Item 25

Request

With regard to Section 4.5.6.2-Containment Drywell Melt-through, please discuss the consistency of your IPE insights with those described in draft NUREG/CR-5423, "The Probability of Liner Failure in a Mark-1 Containment", dated January 1990, (or the more recent final report dated August, 1991.) Discuss the effects of the insights from this most recent work upon the liner failure probabilities shown in Table 4.5.6.1.

Response

A major premise of the JAF back-end analysis was that JAF is very similar to Peach Bottom. In particular, only two important differences were identified that could affect the depth of debris contacting the liner and thus liner melt-through: core mass and drywell sump size.

Several studies[6,7] have concluded that the depth of debris contacting the liner is an important parameter affecting the likelihood of liner melt-through. Clearly for cases in which little debris is released from the vessel and little or no debris reaches the liner, melt-through is highly unlikely or impossible. However, if the depth of debris in contact with the liner is large (i.e., greater than 30 cm), the likelihood of liner melt-through is much greater. Two parameters that can significantly affect the depth of debris in contact with the liner are the mass of corium released from the vessel and the drywell sump volume. The sumps collect the debris and prevent it from spreading across the floor.

Table 4.5.1.1 of the JAF IPE Volume 1, Section 4.5.1 shows that the JAF core is approximately 17 percent smaller than the Peach Bottom core, and thus the mass of core debris released from the vessel following vessel failure will be lower for similar accident sequences. Table 4.5.1.1 also shows the JAF drywell to be roughly the same size as the Peach Bottom drywell. Smaller potential releases into a similarly-sized drywell will result in shallower debris beds on the drywell floor in the JAF plant, and thus the debris bed depth in contact with the liner will be lower.

[6] Theofanous, T. G., et al., "The Probability of Liner Failure in a Mark-I Containment," NUREG/CR-5423, The University of California, August 1991.

[7] Weingardt, J. J. and K. D. Bergeron, "TAC2D Studies of Mark I Containment Drywell Shell Melt-Through," NUREG/CR-5126, Sandia National Laboratories, August 1988.

Furthermore, the JAF drywell sumps have a larger capacity than the Peach Bottom sumps (JAF drywell sumps have a depth of 4 ft and a total free volume of 261.0 ft^3; Peach Bottom drywell sumps have a depth of 1.4 ft and a total free volume of 203.0 ft^3 [8]). When more debris is confined to the sumps, less is available to spread across the floor and contact the shell, reducing the total debris height in contact with the liner in hypothetical accidents.

The two differences between JAF and Peach Bottom would tend to reduce the height of debris in contact with the liner and reduce the likelihood of liner melt-through at JAF. Given this assessment, the Authority felt confident that the expert data from the NUREG-1150 analysis shown in Table 25.1 would overestimate the frequency of large releases attributable to liner melt-through at JAF. However, because this issue is controversial, NUREG-1150 data were applied and the overestimation of large releases accepted.

Table 25.1 Probabilities of Drywell Shell Failure[9]

Case	2 min	5 min	10 min	1 h	2 h	3 h	5 h	10 h	CCI neg*
a Wet	0.00	0.07	0.22	0.32	0.33	0.34	0.34	0.34	0.35
b Dry	0.09	0.19	0.39	0.51	0.53	0.54	0.54	0.54	0.54
c Wet	0.04	0..17	0.32	0.38	0.39	0.39	0.39	0.39	0.39
d Dry	0.21	0.53	.071	0.79	0.80	0.81	0.81	0.81	0.81
e Dry	0.21	0.38	0.51	0.60	0.61	0.61	0.61	0.61	0.61

* indicates time (hours) when core-concrete interactions become negligible

The expert assessment of containment drywell melt-through was summarized into five cases for application to the JAF CET, the probability of drywell liner failure being expressed as a function of the debris flow rate, reactor pressure vessel pressure, extent of metal oxidation, debris superheat, and presence of water on the drywell floor. The five cases addressed in Table 25.1 are:

[8] Theofanous, T. G., Ed. a., "The Probability of Liner Failure in a Mark-I Containment," NUREG/CR-5423, page 23, The University of California, August 1991.

[9] NUREG/CR-4551 Volume 2 Part II, Table 6-2, "Probabilities of Drywell Shell Failure."

[a] Low and medium debris mass flow rates with water on the drywell floor

[b] Low and medium debris mass flow rates without water on the drywell floor

[c] High debris mass flow rates with water on the drywell floor

[d] High debris mass flow rates without water on the drywell floor and with at least two of the other three parameters (reactor pressure vessel pressure, percentage of metal, and debris superheat) high

[e] High debris flow rates without water on the drywell floor and at least two of the other three parameters low.

The parameters were defined as follows:

Debris mass flow rate:	Low	(<50 kg/s)
	Medium	(50 to 100 kg/s)
	High	(>100 kg/s)
Water on drywell floor:	Yes	(replenished)
	No	(not replenished)
Reactor pressure vessel pressure:	High	(1,000 psia)
	Low	(200 psia)
Percentage of metal:	High	(65% zirconium)
	Low	(35% zirconium)
Debris superheat:	High	(>100K)
	Low	(<100K)

Cases a and c reflect wet conditions within the drywell; the other cases reflect dry conditions within the drywell. The term "wet" implies a significant quantity of water is present on the drywell floor. For simplicity, it was assumed that liner melt-through within 10 hours of vessel breach was a form of early drywell failure and could result in a large early release. This treatment is conservative but avoided additional complexity in the source term model. Taking the failure probabilities at 10 hours as being representative of the failure probabilities applied in the analysis, the failure probability for wet cases was roughly 0.37 (the mean of 0.34 and 0.39), and the failure probability for dry cases was roughly 0.65 (the mean of 0.54, 0.81 and 0.61).

In contrast, the probabilistic methodology applied in NUREG /CR-5423 results in predictions that liner failure is "physically unreasonable" for the wet cases, with failure probabilities in the 10^4 to 10^6 range. Liner failure for the dry cases was found to be "virtually certain" with probabilities varying from 0.63 to 1.

Comparing NUREG/CR-5423 data with those used in the JAF IPE indicates that the failure probabilities applied in the JAF IPE for wet drywell cases are orders of magnitude higher than those proposed in NUREG/CR-5423 and that the failure probabilities for the dry cases are essentially the same (they are certainly equivalent given the large uncertainties surrounding this issue). It can therefore be asserted that the data used in the JAF IPE are conservative. Since the probabilities differ significantly for the wet cases but not for the dry cases, we will only discuss implications of the NUREG/CR-5423 data for the wet cases.

Figure 4.7.4.5 in the JAF IPE clearly shows that the dominant mode of early containment failure for all plant damage states (PDS) is drywell melt-through. Thus, reducing the likelihood of drywell melt-through for all wet cases would reduce the frequency of early releases. Given that Figure 4.7.4.3 in the JAF IPE shows that sprays (a dominant source of water for the drywell floor) are not available (early or late) in roughly 60 percent of the PDS-1 sequences, and PDS-1 represents more than one-half of the total core damage frequency, it is clear that use of NUREG/CR-5423 data will result in a marked decrease in the probability of releases.

Finally, it will be recalled that the source terms that result from drywell liner failure in accident sequences involving water on the floor will be lower than for sequences involving a dry drywell because the water pool that quenches the debris and prevents it from causing drywell liner failure is also very effective at scrubbing fission product aerosols from gaseous releases. Spray droplets would also mitigate releases. Therefore, the source terms for the flooded cases would not be in the "high" category. Given reduced frequencies and source terms, the wet cases do not significantly impact overall containment response measures.

However, while the JAF IPE would seem superficially to be very conservative in its handling of the failures of a wet drywell, the adoption of NUREG/CR-5423 data may be inappropriate because NUREG/CR-5423 did not consider basemat ablation and failure of the drywell shell below the sumps--the presence of equipment sumps inside the pedestal was apparently neglected. Debris depths exceeding 2 ft (actual sump heights are 4 ft) are expected in the sumps. This debris is less likely to be cooled by water. Localized molten core-concrete interactions (MCCI) may thus ablate the floor and possibly fail the containment liner which is only a few inches from the bottom of the sumps. Since this failure mechanism was not considered in NUREG/CR-5423, the

Authority feels that the existing quantification of the likelihood of liner failure is appropriate given the levels of uncertainty surrounding the issue.

We can therefore conclude that although the use of NUREG/CR-5423 data would significantly reduce the probability of early containment failure for all wet cases, the majority of accident sequences (as determined by their cumulative frequency) are associated with a dry drywell and would not be affected by the new data. Because the failure data for dry cases presented in NUREG/CR-5423 are essentially the same as the data applied in the JAF back-end analysis the frequency of large early releases would not change significantly. Therefore, application of the new data would reduce the early failure frequency but not the overall severe accident response characterization. Furthermore, data from NUREG/CR-5423 may not be appropriate for JAF. In our judgment, the change in the large release frequency that would result from applying the new data would not represent a significant improvement to the JAF analysis.

Item 26

Request

On page 4-55 in the third line from the top of the page, please identify the starting event for the 24 hr. termination of the analysis of Core Concrete Interactions (CCI), i.e. is the 24 hrs. measured from the start of initiating event, core damage, vessel failure or CCI?

Response

In the core damage sequences and potential CCIs described in the JAF IPE, all times are measured from the occurrence of the initiating event (i.e., in all dominant core damage sequences, the loss of offsite power event). CCIs are followed for 24 hours after initiation of the accident sequence as the release of fission products from containment is essentially complete within 24 hours.

Item 27

Request

Examination of Figures 4.7.4.3 and 4.7.4.5 seem to indicate that for PDS-1 there is a probability of early containment failure of 0.038 from some mechanism other than drywell melt through, drywell over pressure rupture, or wetwell venting. Is this representative of containment bypass leaks (i.e. event V and/or containment isolation failure)? This unidentified mechanism seems to have a frequency of 3.9 x 10^{8}/yr and accounts for 2.1% of all core melt events. Please clarify this and discuss its significance.

Response

Figure 4.7.4.3 shows the impact of drywell spray operation upon the conditional probabilities of early containment failure. The figure therefore reflects all the early containment failure modes. However, Figure 4.7.4.5 presents the conditional probabilities of only the three dominant early containment failure modes. The complete list of these failure modes for PDS-1 is as follows:

Containment Failure Mode	Conditional Probability
Drywell liner melt-through	0.528
Drywell rupture	0.135
Wetwell venting	0.075
Drywell head leak	0.019
Wetwell rupture	0.016
Wetwell leak	0.0022
Drywell leak	0.0002
Total	0.776

No "V" sequence event or containment isolation failure is listed.

Item 28

Request

Generic Letter 88-20 Supplement 1, dated August 29, 1989, requests that BWR licensees with a Mark I Containment design address the specific Mark I Containment Performance Improvements (CPIs) identified in the supplement to GL 88-20 and references 1 and 2 below. Please examine the suggested CPIs and provide your evaluation of the value/impact associated with the suggested improvements and any sensitivity with regard to estimated core damage frequency. (Use references as appropriate.)

Response

BWR Mark I containment performance improvements, discussed in Generic Letter 88-20, Supplement 1, were considered in the JAF IPE. The following CPIs were examined:

- Emergency operating procedures (Revision 4 of the BWR Owners Group Emergency Procedure Guidelines)
- Alternate water supply for vessel injection
- Alternate water supply for drywell spray
- Enhanced reactor pressure vessel depressurization system reliability
- Containment venting.

The manner in which these were addressed in the IPE is as follows.

Emergency Operating Procedures (EOPs).

The EOPs addressed in Revision 4 to the BWR Owners Group Emergency Procedure Guidelines (EPGs) were implemented at JAF in June, 1990 and were incorporated in the JAF IPE event and fault tree models. Because the EOPs reflect the latest generic NRC-approved actions for mitigating potential transients that go beyond the design basis of the plant, the core damage frequency (CDF) predicted is expected to be lower than the CDF based on previous EOPs.

Alternate Water Supply for Vessel Injection.

At JAF, the fire protection system (FPS) can be cross-tied to the residual heat removal service water (RHRSW) "A" header which, in turn, can be cross-tied to the "A" RHR low pressure coolant injection (LPCI) path. The availability of this alternate injection path reduces the CDF associated with loss of injection accident sequences and delays core damage in station blackout sequences. In the JAF IPE study, this use of the FPS had little impact because the dominant sequences initiated by A, S1 and T3C events in which vessel injection failed are dominated by the failure of low pressure emergency core cooling system injection valves to open. Since the FPS uses the same path to inject coolant into the reactor, these failures will also preclude use of the FPS to provide vessel injection.

Use of the FPS diesel-driven fire pump during a SBO event was discussed as a possible mitigating action after battery depletion and loss of dc power and the subsequent loss of high pressure coolant injection using high pressure coolant injection (HPCI) and reactor core isolation cooling (RCIC) systems. It was concluded that use of the FPS during SBO sequences could only delay accident progression as, without ac power recovery, the SRVs cannot maintain low reactor pressure and so assure continued FPS operation. Furthermore, even if reactor depressurization is assured through an alternate dc power supply, without ac power recovery, systems required for containment decay heat removal will still be unavailable. The resulting high containment pressures exerted on the SRVs will cause their closure. The subsequent rise in reactor vessel pressure to a value above the FPS pumps shutoff head precludes reactor vessel make-up.

Although the CPIs only address the use of an alternate water supply for vessel injection, other uses are possible for this supply. Loss of containment heat removal (TW) sequences that result from RHRSW pump failure can be recovered by manually aligning the FPS pumps to the discharge of RHRSW header A to remove decay heat from RHR heat exchanger A. This use of the FPS reduces the probability of core damage in TW sequences. While the manual alignment of the FPS to the RHR system via the RHRSW heater A is currently addressed in the procedures, it is only to provide an alternate reactor injection source. Therefore, the Authority is now considering modifying the procedures and operator training to allow manual alignment to the discharge of RHRSW header A.

Modification of the FPS to allow it to provide EDG jacket water cooling through the ESW system is also under consideration. This modification would reduce the SBO core damage frequency because the leading contributor to SBO events and internal CDF is the unavailability of the emergency service water (ESW) pumps and the resulting loss of cooling and failure of emergency diesel generators (EDGs).

Alternate Water Supply for Drywell Spray.

It has yet to be resolved whether fire protection system pumps can provide the necessary discharge for adequate flow to the drywell spray headers at JAF. Nevertheless, the JAF IPE did examine the benefits of drywell spray operation during the accident progression and their effects on containment performance. The conclusions of this examination are summarized in the JAF IPE, Volume 1, Section 4.9.3. In summary, drywell spray operation:

- Reduces the probability of containment failure because water on the drywell floor reduces the likelihood of drywell liner melt-through and, because the sprays reduce containment pressure, lessens the probability of static overpressurization.
- Delays containment failure by reducing the likelihood of drywell liner melt-through. This delay will reduce the radiological source term because natural decontamination mechanisms will have more time to act prior to containment failure.
- Shifts the location of containment failure from drywell areas to the wetwell by reducing the likelihood of drywell liner melt-through. Again, this shift will reduce the radiological source term because releases from containment will be scrubbed by the suppression pool.
- Enhances fission product decontamination by direct scrubbing of fission product aerosols and increasing residence time within containment by decreasing pressures and thus the outflow rate from containment. The increased residence time enhances the effectiveness of natural decontamination mechanisms.

Enhanced Reactor Pressure Vessel (RPV) Depressurization System Reliability.

The effects of enhanced RPV depressurization system reliability were not directly quantified in the JAF IPE. However, the examination of the JAF plant damage state accident progressions and phenomena show the beneficial effects of enhanced RPV system reliability. For example, examination of the plant damage states indicates that RPV low pressure accident progressions are less likely to result in early containment failure--in PDS-2, a low-pressure SBO scenario, the conditional probability of early containment failure is 0.57 whereas in PDS-1 the probability of containment failure is 0.78. This difference arises because low pressure core melt progressions are less likely to result in containment failure at vessel breach than are high pressure melt progressions and are thus expected to reduce source terms by an order of magnitude[10].

The Authority has examined the provision of a portable generator to charge the dc batteries and so ennance the reliability of the RPV depressurization system and thus the ability of the plant to cope with an SBO. It was felt, however, that a reduction in CDF could be better achieved through other changes (e.g., use of a fire-water cross-tie to the ESW system to provide EDG jacket cooling).

Enhancements to RPV depressurization system reliability could also increase the likelihood of maintaining reactor coolant injection. The ability to use low pressure core cooling systems to inject reactor coolant depends on the safety relief valves (SRVs) maintaining reactor vessel pressure below the shut-off head of the low pressure core cooling system pumps. However, in TW sequences, the SRVs will not stay open because as containment (drywell) pressure approaches the 80-psig pneumatic system pressure, the SRVs are forced closed. Subsequently, the reactor vessel will repressurize precluding make-up using low pressure core cooling systems. This accident phenomenon also affects use of the FPS during an SBO event.

The Authority evaluated the feasibility of increasing nitrogen supply pressure above the containment failure pressure to sustain SRV operability in these scenarios. However, it was decided that other changes to reduce the CDF were more practical.

Containment Venting.

Containment venting was addressed in the JAF IPE as a means of preventing catastrophic containment failure and mitigating the consequences resulting from a severe core melt progression.

The JAF containment vent path consists of hard piping from the containment to the inlet transition piece of the standby gas treatment (SBGT) system filter train. Because this transition piece is located outside the reactor building pressure boundary, failure of the transition piece upon containment venting will only fail the SBGT system. Loss of the SBGT system will not increase core damage frequency. Therefore, the survivability and accessibility of vital plant equipment are not compromised by releases within the SBGT room upon containment venting.

Containment venting was examined for three types of accident sequences:

[10] Herschel Specter and Peter Bienarz, "Is Mark 1 Shell Failure Really Important? Part Two," Nuclear Engineering and Design 121 (1990) 447-458.

- Long-term loss of containment heat removal (TW) sequences
- Anticipated transient without scram (ATWS) sequences
- Station blackout (SBO) sequences.

The containment venting scenarios for these sequences will now be described.

Long-Term Loss of Containment Heat Removal (TW) Sequences.

A plant transient with subsequent loss of normal decay heat removal by both the turbine bypass valves (to the main condenser) and residual heat removal (RHR) system (suppression pool cooling, drywell spray, etc.) results in rising containment pressure. Eventually (after 20 hours), containment pressure approaches the 44-psig primary containment pressure limit (PCPL). By venting the containment at this time using the wetwell venting pathway, containment overpressurization is prevented. The containment will remain vented until a normal decay heat removal pathway is restored or the pressure is reduced.

If containment venting fails, the high containment pressure exerted on the SRVs will cause their closure. The reactor vessel pressure will then rise above the low pressure emergency core cooling system pump shut-off head. Because high containment pressure will trip RCIC on high turbine exhaust pressure, core damage will ensue if HPCI is unavailable. Otherwise, containment failure will precede core damage and increase the potential for core damage caused by the harsh reactor building environment.

The risk importance of containment venting for the JAF IPE is calculated by comparing the total CDF with and without containment venting. Assuming that containment overpressurization leads to a loss of core cooling, the following CDFs can be calculated using JAF IPE results:

CDF, without venting	=	2.72×10^{-5}/yr.
CDF, with venting	=	1.92×10^{-6}/yr.

The total CDF resulting from internal events is reduced by a factor of 14 because of containment venting during TW sequences--venting during TW sequences is an important mitigating action.

Anticipated Transient Without Scram (ATWS) Sequences.

Containment pressure is expected to rise above the PCPL at an early stage in certain ATWS accident progressions. In the JAF IPE, containment venting was considered only for those ATWS sequences in which successful boron injection (and hence a lower reactor power level) and loss of long-term containment decay heat removal occur. Containment venting is ineffective in ATWS sequences that involve boron injection failure because the resulting high reactor power level would exceed the capability of all containment vent paths. However, because the ATWS initiator frequency is low, the expected frequency of sequences requiring containment venting is low and therefore the impact of containment venting on the CDF predicted for ATWS events is negligible.

Station Blackout (SBO) Sequences.

A SBO involves a plant transient in which all sources of ac electrical power are unavailable. The reactor is shut down; only the steam driven HPCI and RCIC systems are available for reactor level control. As with TW sequences, containment pressurization occurs slowly. Because the HPCI and RCIC systems depend on dc control power, battery depletion leads to their failure. Without ac power recovery, core water boil-off and core damage ensue. Because the core melt progression and vessel breach occur before the PCPL is reached, containment venting is not performed. However, two containment venting strategies were considered in the JAF IPE containment performance analysis: the local alignment of wetwell venting during core degradation (in SBO core degradation progressions, a 10 percent success rate was assumed) and wetwell venting when containment pressure exceeds the PCPL.

The impact of these two venting strategies on the JAF plant damage states accident progressions is compared in the JAF IPE, Volume 1, Section 4.9.3. The insights gained from this comparison are:

- Containment venting does not preclude drywell liner melt-through.

- Containment venting through the wetwell pathway is a controlled release intended to relieve containment pressure and prevent or delay gross containment rupture during and after vessel breach.

- Wetwell venting will scrub the evolved gases in the suppression pool and reduce the fission products released from containment.

It should be noted, however, that because containment venting is itself defined as one mode of containment failure, the overall likelihood of containment failure increases when the operators can, and are instructed by procedure to, vent the containment if containment pressure reaches the PCPL.

Item 29

Request

Please discuss the containment walkdowns performed to confirm that the IPE represents the as-built, as currently operated plant. Please identify the operations staff and level-2 experts who participated in containment walkdowns.

Response

A review of plant systems located inside containment identified no equipment or hardware that affected the containment back-end analysis. Therefore, efforts were concentrated on identifying fission product release paths that might bypass the containment or reactor building. This entailed a detailed review of general arrangement, structural and floor planning drawings for the drywell, torus (wetwell) and reactor building (secondary containment) structures. In addition, the team spent one day performing a containment "walk-through" using a comprehensive laser-disk based photograph library. From these reviews, it was concluded that a violent interaction between core debris and the torus water inventory could occur if the downcomers were level to or slightly above the drywell floor elevation. To determine the position of the downcomers thoroughly, physical observation was required. In keeping with ALARA philosophy, containment walkdown by the entire level-2 team was deemed unnecessary and was therefore not performed. However, a containment walkdown was performed by plant personnel to determine the height of the downcomers above the drywell floor.

In addition to the walkdowns performed specifically for the containment analysis, numerous walkdowns of the reactor building were performed as part of the level-1 internal flooding analysis. These walkdowns paid particular attention to crescent area configuration and any open equipment hatchway pathway inside the reactor building. These walkdowns in turn proved useful in identifying fission product release paths.

The level-2 experts who reviewed plant drawings and the laser-disk based photo library, were John Favara and Andrew Mihalik of the New York Power Authority and Chris Amos and Jay Weingardt of Science Applications International Corporation.