Lawrence Livermore National Laboratory

NUCLEAR SYSTEMS SAFETY PROGRAM

August 13, 1984
EM-84-138/DDA

Ms. Sarah Davis
Reliability and Risk Assessment Branch
Division of Safety Technology
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D. C. 20555

SUBJECT: First Round Questions on the Seabrook Station PRA

Dear Ms. Davis:

The attached set of questions on the Seabrook PRA are the result of our preliminary work on the PRA review.

The questions cover a number of areas, and range from very detailed to modestly general. We have attempted to concentrate on questions that have a potential for being important, or are important to the results. However, some of these questions may eventually be shown to be unimportant, since there is no way to predict where some of the answers may lead us.

As you know, we desire to discuss these questions with the plant and/or utility personnel during the plant visit planned for the last week in August. If you are able to send them a copy prior to the visit, it would probably improve the likelihood of fruitful discussions during the visit. It should be noted that this set of questions are only our first round questions, and that we may identify additional questions prior to, during, or following the plant visit. If it is possible, it would also be desirable to identify a key person at the plant/utility so that questions may be processed quickly. This will become even more important later as the project approaches completion.

If you should like to discuss any of these questions, please call me directly.

Sincerely,

Abel A. Garcia

Abel A. Garcia
Principal Investigator
Seabrook PRA Review Project

AAG/sa

FOIA-87-006
B/14.

Enclosure

cc: L. L. Cleland/G. E. Cummings

# FIRST ROUND QUESTIONS ON THE SEABROOK STATION PRA

August 7, 1984

## A. INITIATING EVENTS

1. Provide a copy of sheet 5 of Table 5.2-4 from the report, if it exists, so that our evaluation of support system initiators can be completed.

2. Transient event Categories 7 through 16 appear to have similar or identical plant responses, with the major difference being that some transients affect the operation of the PCS (defined as the main steam, condenser steam dump, condenser, condensate, and feedwater systems). It therefore appears reasonable to reorganize these ten categories into only two categories: One with PCS available, the other with PCS not available.

Answer the following questions for each of these event categories (7-16):

a. Will all four of the MSIVs receive "close" signals as a direct result of this transient initiator? Why or why not?

b. Will a safety injection signal occur as a direct result of this transient initiator? Why or why not?

c. Can the PCS (as defined above-normal cooling cycle without aux. feed) be utilized to cool down the plant for this transient initiator?

When answering, assume that the event is in its early stages and and that no other system failures have occurred other than those caused by the initiating event.

c. Answer these same questions for a steam generator tube rupture event.

3. There has been some concern at certain plants about an initiator known as an "incore instrument tube rupture event". The salient feature of this event is that it is a LOCA which discharges into the reactor cavity and not into the containment sump. Thus, if containment sprays are not available by the time recirculation is required, a dry sump condition exists which would result in failure of recirculation. Why is it not necessary to consider this type of initiator for Seabrook?

4. Other PRAs have included loss of a vital AC bus as an initiator and found it to be among the dominant contributors to core melt. Why is it not necessary to consider this initiator for Seabrook?

B. EVENT TREES

Transients:

1. The text states that it is possible to avoid the need for recirculation in bleed and feed scenarios by initiating closed loop RHR cooling. However, it appears that no credit is taken for this in the event tree; all bleed and feed sequences end in high pressure recirculation. Which way was this sequence actually analyzed in the study? If it was the former, provide further justification for this position since it appears to be an optimistic view of the scenario.

2. Why was turbine trip combined with MSIV closure and PCS cooling combined with auxiliary feedwater cooling? These combined events do not correctly represent the plant sequence. We believe that four events are required to evaluate the situation properly: First would be turbine trip, followed by PCS, then MSIV, and finally aux. feed. PCS would be considered only if turbine trip succeeded. Preventing overcooling by turbine trip versus MSIV closure is not equivalent in the plant response, thus they should not be included in the same event.

3. Why does the tree not include an event for the transient induced small LOCA (transient followed by a stuck open PORV)? This event has been considered in all previous PRAs.

4. Why is it necessary to consider the separate event OM for control of feedwater to prevent overcooling? The important action is that HPI be controlled whether or not feedwater is, or PTS will occur. Explain the need for a difference in the tree structure based on the failure or success of event OM.

5. What is the basis for a need for plant stabilization and cooldown within 24 hours when auxiliary feedwater is operating? Your analysis is based on the limit of 200,000 gallons of CST water which is "reserved" for AFW. We have two problems with this. First, it seems unreasonable to assume that additional water would not be available in this 400,000 gallon tank. Even if this is not "reserved" for AFWS, why couldn't it be used for AFWS? Second, no credit is given for the water in the steam generators. The additional 89 FPS (full power seconds) in this water (by your own analysis) would extend the time frame for loss of all secondary cooling to about 24 hours. The event ON, in this case, appears to be extraneous and conservative.

6. We disagree that the use of event ON as described for the RCP LOCA case will change an early melt to a late melt. Your analysis of the RCP LOCA case in Appendix B is not consistent with NRC analyses of time to uncovery. Although we agree that depressurization in a timely fashion will slow the leak rate somewhat, you have not provided justification that demonstrates a large effect. We would agree, however, that if ON were redefined to require success of low pressure injection in some form, the result would be a late melt. Provide justification for your position.

7. Why would a failure of TT with failure of the operator to control feedwater and failure of either RWST or HPI result in a core melt? We would argue that the feedwater flow would provide sufficient

cooling. Although overcooling is expected, this has never been assumed to lead to core melt. Please explain the basis for this very conservative assumption.

Long Term:

8. Why is the air purge isolation a GS where containment isolation succeeds and an IC where containment isolation fails and sprays are operating? These events are not adequately defined in the text and the distinction made between these two systems and the effects of their failure is not explained. Provide justification for the model as evaluated.

Small LOCA:

9. It is stated that recirculation is not required if steam generator cooling and a RCP are available during injection (cooling can be supplied directly by RHR). This is not reasonable, since break flow would not be completely terminated and RHR does not provide make-up. We have seen no analysis that shows this to be possible. In fact, an analysis which attempted to demonstrate that recirculation was not required within 24 hours for Millstone 3 did not support the claim despite that plant's very large RWST and substantial credit for operator action to conserve RWST inventory. Unless suitable analysis demonstrating the contrary is provided, we must conclude that recirculation should be required for all small LOCA cases.

10. If the operator erroneously concludes that he no longer requires HPI for cooling, is it possible for him to terminate it? Under what conditions? If the plant then returns to an insufficient cooling condition, will HPI then restart automatically?

11. Provide copies of the emergency procedure guidelines concerned with response to pressurized thermal shock (PTS). Also provide copies of any other procedure guidelines (or procedures, if prepared) involving the termination and/or manual control of high pressure injection or

feedwater.

12. The assumption that failure to control auxiliary feedwater given a small LOCA and TT failure will result in eventual loss of all feedwater appears very conservative. What would cause this loss?

Medium LOCA:

13. The text refers to the use of condenser steam dump during medium LOCA. Isn't this system lost due to MSIV closure following the safety injection system? How was this analyzed in the study?

14. Why is operator depressurization (event OD) considered even if HPI is available? Why would he try this if he had HPI cooling? Why is auxiliary feedwater considered when HPI is available, since it is not required? It appears that these sequences are not necessary: they confuse the analysis and create additional unnecessary entry states into the long term trees. Explain why the additional sequences are necessary and describe how they affect the analysis.

15. Why do sequences where injection phase cooling succeeds and the RHR pumps fail lead to an early melt? The text states that the depletion of the RWST would determine when melt occurs for this case. For the case where the RWST valves fail closed, a late melt is assumed. This contradiction requires an explanation.

Large LOCA:

16. Justify the assumption that there will be no damage to the RHR or CBS pumps during recirculation if the RWST suction valves are not closed? Is there no possibility that the RWST suction line would completely drain and result in the intrusion of air into the pump suction lines and subsequent pump cavitation? Why isn't this same assumption applied to the other trees (at least it isn't discussed)? In general, explain how this was treated throughout the analysis.

17. What is the basis for the need to switch to hot leg recirculation? Is this need a real issue or the result of the use of conservative licensing analysis?

18. Events LA and LB on the large LOCA tree are described as being identical but of opposite trains. This is incorrect since both of these events include the accumulators, which have no opposite train. These events are actually conditional, with success of LB being dependent on whether or not LA has failed and how it has failed. The accumulators should have been handled as a separate event. Explain how the analysis was handled to account for the dependence of these events.

19. In the sequences where the containment enclosure building ventilation system fails (e.g., sequences numbered 94-102), why are there decision points for both of the RHR trains? The plant damage states are shown as being identical for all cases so that the sequences appear to be redundant and extraneous, adding nothing to the insights from the analysis. Wouldn't GF for these systems be more appropriate?

20. Why is the containment enclosure building ventilation system included directly on this tree? Isn't inclusion as a support system state (EH) sufficient? If not, why is this important only on the large LOCA tree? Shouldn't it also be included on the other long term trees since long term ventilation would always be required for long recirculation periods? Finally, other studies have shown that these ventilation systems often provide only a habitability function, and that they have no effect on the operability of the systems they ventilate. Is the requirement for ventilation simply a conservative assumption or is it based on analysis? Was direct cooling of the pump and/or cooling by the working fluid considered?

Steam Line Break:

(Outside Containment)

21. For those cases where MSIV closure and AFWS succeed, why is there a decision point for HPI? Given that HPI will be commanded to start, why is this significant? How does this affect the eventual plant condition?

(Inside Containment)

22. Why is there a need for boron injection when auxiliary feedwater works? Is a potential return to criticality a valid concern? On what basis? Even if it is, why is recirculation considered (RCS fluid is not being lost since there is no nonisolable break)? What is the basis for modeling a significant difference in plant response between steamline breaks inside and outside containment? The differences in the trees appear to be artifacts of the analysis. Is this the case?

Steam Generator Tube Rupture:

General Comment: The SGTR tree is very poorly arranged and appears to reflect a significant lack of understanding of the event. The extent of the specific questions and comments below indicate that consideration should be given to the construction of a completely new tree.

23. What is the basis for concluding that the RWST will not empty until 24 hours? Your analysis of LOCAs does not provide a basis for this conclusion, even assuming a higher downstream pressure. It is not apparent that the flow rate for the high pressure systems will be reduced sufficiently to extend injection to 24 hours.

24. You have assumed that control of HPI flow is required only under certain conditions. Provide justification for assuming that control of HPI is not required for all cases. We would hold that failure to

control HPI would result in RCS pressure being held high while simultaneously pumping the entire volume of the RWST into the RCS and thus into the secondary, leaving no water for cooling and continued break flow, and resulting in eventual core melt. This is partially covered by event OR, except that the event definition should include the operator controlling HPI and failure of this event should always lead to core melt.

25. Provide copies of all emergency procedure guidelines pertaining to SGTR.

26. Why is event ON required? This event appears to increase the number of sequences without providing additional insights. The concept of "long term industry response" is not explained in any context which gives it any substance; it appears to be superflous. For the RCP LOCA case, "limiting damage to the seals" is a mildly optimistic concept at best, and we would question any perceived change in plant damage state from this action without more formal justification. (We also note a typographical error on the tree for this case. According to your nomenclature, the ON failure branch should be labeled K', not K.)

27. What is the justification for the assumption that failure of both auxiliary feedwater and bleed-and-feed results in a late melt due to the effects of the steam generator inventory? This result is directly in conflict with the results for similar sequences on both the small LOCA and transient trees. In those events, loss of both AFWS and bleed and feed always results in an early melt (an assumption which has always been made in previous PRAs). Since a SGTR event is roughly "between" a transient and a small LOCA, a similarity in the timing of core melt for similar sequences would be expected.

28. What is the justification for assuming that it is possible to avoid core melt when HPI is unavailable and a steam leak occurs? How would break flow be stopped (downstream pressure would be atmospheric)?

While event OD would delay melt, the occurrence of the steam leak would change this event from a controllable SGTR to an uncontrollable interfacing systems LOCA (a classic case) such that at the conclusion of injection there would be no water available for recirculation and a core melt would result.

## C. SUCCESS CRITERIA

1. What is the basis for the 3/4 success criteria for MSIV closure for transient events? (i.e., What is the justification for saying that the blowdown of only one steam generator cannot result in a PTS demand?)

2. The difference in pressure and flow rate of the charging pumps versus the safety injection pumps leads to a question for the small LOCA HPI success criteria: Are there any break sizes within the small LOCA range where any one-out-of-four pumps is not sufficient? (i.e., where one CP is not success due to insufficient flow or one SIP is not success due to an insufficient reduction in RCS pressure.)

3. What is the justification for the ECCS success criteria for medium LOCA. This criteria is contrary to that found in most previous PRAs on similar plants. Why isn't there a need for accumulators? Is HPI success <u>any</u> two-out-of-four pumps? The respective flow rates of the CP and SIP do not support this. We note, however, a good deal of confusion regarding flow rates: the success criteria analysis in Appendix B assumes identical and quite high flow rates for all these pumps for the purpose of RWST depletion. These high flow rates would be very optimistic if applied to success criteria for ECCS cooling. What was really done?

4. Provide justification for an SLBI success criteria which requires three-out-of-four MSIVs to close. We believe the correct criteria for preventing multiple SG blowdown should be three-out-of-three MSIVs on the unaffected SGs or one-out-of-one MSIV on the affected SG.

D. HUMAN ACTION

General Comment: The report does not make clear how these trees were quantified, what values were used for each branch of the trees, and where they are from. This should have been explicitly included in the report so that the results would be reproducible.

1. The need for event OH in ten minutes seems in general to be very conservative for most ATWS cases. In the absence of a LOCA, if the plant rides through the initial phase of the ATWS and is on auxiliary feedwater, we would expect the plant to have reached a semi-stable condition so that OH would only be required in the long term (>60 minutes) to provide boration for eventual shutdown. If a LOCA condition exists, the need to supply makeup flow overrides other considerations and a shorter time frame (on the order of 20 minutes) would be reasonable. Why was the assumption made? Would the descriptions above more accurately describe the two cases?

2. Justify consideration in the report of a diagnosis phase for event RT. In this conservative approach, diagnosis implies that the operator attempts to determine that there is a need for a manual trip before pressing the manual trip buttons. This is not the case: manual trip is normally a reflex action performed by the operator in response to serious abnormal conditions without any attempt to diagnose the precise conditions present, thus, his response would not be expected to be based on a cognitive error model.

3. For events RT and OH, should the distribution shown on page 10.3-7 be for end state 3 (failure to perform trip), rather than for end state 1 as stated in the text? It appears to be in conflict with Table 10.1-1.

4. For event OM the report concludes that complete termination of auxiliary feedwater flow is acceptable. We would expect a requirement for some feedwater flow to prevent boil dry. What is the

basis for the conclusion that this end state is acceptable?

5. For event OM, why are overcooling and boil dry considered the same end state? We would expect that boil dry could lead directly to core melt but that overcooling only leads to a potential PTS.

6. For event OP, explain how this analysis deals with the PTS problem and related action.

7. For event OP, should the reference to end state 2 in the quantification (page 10.3-5) actually be end state 3?

8. For event OP, what is meant by "ask bleed-and-feed" for the failure to take action branch, and what purpose does it serve? This is not made clear in the text.

9. The 2 hour time frame for bleed-and-feed (event OR) appears to be very optimistic. Previous PRAs have usually used much shorter time frames for this action. What is the basis for using this time frame?

10. The 1 hour time frame for action OD2 appears to be optimistic. Previous PRAs have used time frames on the order of 1/2 hour. What is the basis for using this time frame?

11. The analysis of event OP postulates various errors which could lead to loss of HPI from "overcontrolling". The analysis, however, does not include the case of controlling HPI when it should not be done, i.e., when the operator erroneously believes that OP is called for. An example of this would be the case of a small LOCA with both HPI and AFWS operating, so that the plant appears to be stable and the operator concludes he has something like an inadvertent HPI or possibly an overcooling transient (no LOCA). He thus takes action to terminate HPI and does not realize his error until it is too late. It is not apparent that this case is treated in the human factors or event tree analysis, although it is alluded to by the "confusion matrix". Were these potential failure modes treated in the

analysis? If so, how and where?

12. Are SGTR events OP41, OP42, OP51, and OP52 actually versions of event OD on the event trees? If action OP53 (pg 10.3-24) actually exists (i.e., if it is not a typographical error), what is it? The analysis of all these events is generally incomplete and the submittal of any available additional information is requested for use in evaluating their quantification. In addition, how was the possibility of the operator misdiagnosing the plant status and trying the wrong version of OD considered?

E. SYSTEMS:

1. The emergency diesel generators are described as both air-cooled and water cooled (from the service water system). Which is correct?

2. If the preferred pumps in the SWS and PCC trains fail to start when connected to emergency power (following LOSP), is an automatic start attempted for the stand-by pumps?

3. What is the basis for the 20 gpm leakage rate for 10 hrs. followed by a 300 gpm rate following reactor pump seal failure?

4. The calculations for system unavailabilities appear to contain numerous discrepancies. The results presented in Chapter 7 in many cases cannot be reproduced using the equations, block definitions, and component failure data supplied. One example is described below.

   In the electric power system, block RBE5 appears in Figure D.2-11 and is defined in Table D.2-7 as being the "supply breaker from RAT A to Bus E5". The equation describing this block is given on p. D.2-33 as: QH(RBE5) = D + E + F. The failure descriptions for the letter designators appear on p. D.2-32, and the accompanying hardware failure data (listed in Table D.2-8) are:

D - Breaker $\geq$ 480 V fails to open on demand; $6.49 \times 10^{-4}$/d

E - Breaker $\geq$ 480 V fails to close on demand; $1.61 \times 10^{-3}$/d

F - Breaker $\geq$ 480 V fails within 26 hours; $8.28 \times 10^{-7}$/h

(Note: we assume 26 should be 24, but this is not material to the point.

Then D corresponds to the UAT breakers which must open, E corresponds to the RAT breakers which must close, and F corresponds to the RAT breakers which must remain closed for 24 hours.

Evaluating the equation:

$$\begin{aligned} QH(RBE5) = D + E + F &= (6.49 \times 10^{-4}) + (1.61 \times 10^{-3}) \\ &\quad + (8.28 \times 10^{-7}/h)\ (24\ h) \\ &= 2.28 \times 10^{-3} \end{aligned}$$

This should correspond to the result in Table D.2-10 (p. D.2-60), which gives a mean value of $1.63 \times 10^{-3}$ for this block so that our result is 40% larger. No explanation is provided in the text that would account for such a difference, and it is not apparent that this difference might be due to consideration of recovery, etc. We also note that the value in the Table can be arrived at by dropping the "D" term from the equation. Why does this difference in the calculated and listed results exist?

5. The report (p. D.2-4 and -5) states that both unit auxiliary transformers (UATs) and both reserve auxiliary transformers (RATs) will trip together if the protective relays trip one of the pair. In other words, failure trips both UATs or RATs causing the loss of a power source in both trains. However, the reliability block diagram for Class 1E power (Figure D.2-11, p. D.2-76) shows independence between each UAT and between each RAT. The equation for system failure with offsite power available (EP(1) on p. D.2-30) also

assumes independence among all the auxiliary transformers, thus ignoring the dependence between the two UATs and the two RATs. No common cause term appears for this case in Table 7.2-1 on p. 7.2-4. Why are these dependencies not accounted for, particularly for the loss of offsite power cases?

6. In Section D.2-1 (p. D.2-2), the second operability state analyzed is "power available for 6 hours following the initiating event, with no offsite power available". Why is the time criterion 6 hours rather than 24 hours as in the offsite power available case?

7. Explain the apparent contradiction in the following statements (which concern the service water system): Section D.3.1.4.2.2 (p. D.3-9) states "loss of either service water flow train during normal power operation requires unit shutdown", and Section D.3.1.4.3 (p. D.3-10) states "loss of a single train of SW will enable plant operation at reduced power". Provide the technical specifications for the service water system.

8. Either normal PAH ventilation or the PAH ventilation subsystem must function for component cooling system success. The assumption that "normal PAH ventilation is available when offsite power is available" (Section D.4.1.1, p. D.4-1) has the effect of neglecting both ventilation systems for all cases except loss of offsite power (1B and 2B). Was the unavailability of normal PAH ventilation quantified to justify this assumption? What was the result?

9. The pneumatically operated main feed isolation valves are described as failing in the closed position, which could result in a loss of feedwater transient. However, on Table D.5-4 it is stated that they have a "no fail position". What is the actual failure mode of these valves?

10. In general, in the IA system, the failure probability of an IA header does not represent the failure of air supply to a particular component. The failure to supply air to a particular component is

also dependent on the number of isolation valves and filters between the header and that component. How was the contribution of the isolation valves and/or filters in the air feed lines to the pneumatic components analyzed? How was the contribution from human error leaving an isolation valve in closed position evaluated?

11. The reliability block diagram in Figure D.6-5 does not accurately describe the SSPS system for analysis purposes. The instrument channel will produce a signal upon loss of the AC instrument bus (Section D.6.1.3.2.2). Why is the AC power supply modeled to produce failure of each instrument channel? The logic circuit and output relay will fail to trip the ESFAS master relays upon loss of DC power. The ESFAS master relays will fail to trip the slave relays on loss of AC power. Are the AC slave relays powered by the same source as the master relays? By including AC power in both the instrument channel and the ESFAS relays, are you double counting the effect of AC power on the analysis of each train?

12. The quantification of each SSPS instrument channel includes the failure of both input relays (Figure D.7-6). However, each SSPS train (A & B) is only dependent on the activation of one relay. Therefore, the logic circuit block should include both the input and the output relays. What is the difference in the unavailability of an SSPS train if you consider only one input relay? Did you consider the output relay in the quantification of the logic circuit or is it implicitly included in the failure data?

13. Numerous valves are listed as part of the supercomponent blocks that do not appear on the schematics presented. For example, MV-RH-33 on page D.8-1 does not appear on Figure D.8-1. In addition, there are valves shown on the referenced P&IDs that do not appear in the block descriptions or on the schematics (e.g., IA filters, BIT valves). What is the basis for excluding these components from the analysis?

14. Can the opening of the MOV's on the boron injection tank (BIT) bypass line (V846 & V847) fail high pressure concentrated borated water injection?

15. How would failures of the activation or control systems for the ARV valves (in the secondary cooling analysis) affect the unavailability of these valves?

F. DATA AND EVALUATION:

1. What is the basis for assuming that passive components are not susceptible to common cause failures? What is the SSPSA definition of passive components?

2. It does not appear that the V-sequence probability assessment (Sect. 6.6.3.2) is correct based on the valve rupture data given in Table 6.2-1. Can more detail be provided?

G. SEISMIC:

1. Why was failure of interconnected piping between structures due to sliding not considered in the seismic analysis?