JUL 3 1980

50-302

MEMORANDUM FOR: Joseph Murphy, Probabilistic Analysis Staff
Office of Nuclear Regulatory Research

FROM: Patrick O. O'Reilly, Reliability and Risk Assessment Branch
Division of Safety Technology, NRR

SUBJECT: ADDITIONAL COMMENTS REGARDING CRYSTAL RIVER 3 SAFETY STUDY REPORT

In my June 16, 1980 memorandum, I indicated that I might have further comments on the Crystal River 3 Safety Study report. Since I was away from the office last week attending a training course, I was unable to document them until now. However, I believe that most of them were discussed during the meetings you conducted on June 17, and 13, 1980 with SAI and FPC. Besides a number of additional comments, Enclosures 1 and 2 also contain my original comments as provided in my June 16, 1980 memorandum. For the information of those on distribution, Enclosure 1 contains substantive comments regarding the report, whereas Enclosure 2 consists of a number of editorial comments.

ORIGINAL SIGNED BY:

Patrick O. O'Reilly
Reliability and Risk Assessment Branch
Division of Safety Technology
Office of Nuclear Reactor Regulation

Enclosures: As stated

cc;w/Enclosure 1
R. Benero
R. Mattson
F. Rowsome
M. Ernst
G. Edison
S. Israel
F. Coffman
M. Cunningham
J. Curry
F. Manning
H. Ornstein
J. Pittman
M. Taylor
A. Thadani

DISTIBUTION
~~Docket Control~~ File
NRR r/f
RRAB r/f
P. O'Reilly

OFFICE ►	RRAB					
SURNAME ►	P. O'Reilly:ah					
DATE ►	7/03 /80					

NRC Form 318A (4-79) NRCM 0240 ★ U.S. GOVERNMENT PRINTING OFFICE 1979 — 289-369

8008080131 P

JUL 3 1980

ENCLOSURE 1

Comments on Crystal River-3 Safety

Study Working Draft - 5/9/80

General Comment: Define abbreviations the first time used.

Volume 1 - Main Report

Page 2-3: Under item (1), second bullet, what is the basis for stating that it is considered extremely unlikely that the relief and/or safety valves (underline added) will fail to lift near their setpoints?

Under item (2), first bullet, provide the reference for the B&W analysis which shows that, if the EFS does not start automatically, the operator has approximately 20 minutes to manually start it to prevent the safety valves from lifting. It was our impression that the PORV opens early in the case of a LOFW with failure of EFS to auto-start. This would imply that the safety valves would be challenged before 20 minutes into the transient.

Under Item (2), second bullet, according to the analysis reported in NUREG-0565, other operator action is required at about 40 minutes into the transient. Was this additional operator action considered when the decision was made to eliminate this set of transient-induced LOCAs from consideration?

Under item (2), last paragraph, it is difficult to understand the statement about how the sequence can occur, especially in light of additional required operator action at 40 minutes, as discussed previously.

Pages 2-3 & 2-4: Under ATWS sequences resulting in core melt, we question the decision to omit these sequences from consideration. Our specific comments are as follows:

(1) Early B&W analyses (BAW-10099) showed the calculated pressures during an ATWS event to be quite high, in fact in excess of 4000 psig (these analyses did not assume any additional single failures).

(2) What are the bases for the conclusions that:

(a) RCS integrity will be maintained?

(b) Integrity of safety and relief valves will be maintained?

(c) Pump and vessel head seals will not fail?

(d) Steam generator tubes will not fail?

(e) Instruments will remain functional to guide operator actions?

(3) What discontinuities exist regarding item (2) and above and what inelastic analyses were performed?

(4) What is meant by the statement, "Information supplied by B&W...," in the second bullet? Why wasn't NRR assistance in this matter requested, especially since we have extensively reviewed B&W-designed PWR response to ATWS events?

(5) Did the author-contractor also perform work for EPRI on this same subject? If so, there is a possible conflict of interest question because EPRI has espoused the industry position on ATWS.

(6) Provide the basis for the conclusion that a common mode failure that would disable the RPS (resulting in an ATWS event) has relatively low enough probability? What studies were conducted to determine which common mode failures would fail the RPS as well as engineered safety features (e.g., the EFS)? What models were used to estimate the probabilities of these events?

(7) Once the safety valves open during an ATWS event, since they will be exposed to high pressures (7400 psig) and an environment for which they are not qualified, why have they been expected to reclose? In other words, why have ATWS and failed-open safety valves been treated as independent events?

(8) In view of the recent event involving the scram system malfunction at the Browns Ferry Plant, how can it be concluded that ATWS sequences leading to core melt can be omitted from further consideration without providing any bases (other than a statement that they are not significant contributors to risk) for such a conclusion?

Page 2-4: Why is Table 2.2 referred to first, before Table 2.1? Should put tables in same order as they are referred to in text.

Page 2-4: Second paragraph - Were any required automatic or manual actions considered? How much time was assumed for any such actions? What values were assumed for human error and on what basis? If a time limit was assumed for operator actions, what was the basis for it? In these analyses, were longer steam generator dryout times used for the sequences involving loss of offsite power?

Page 2-6 - $B4S_2$ -€ - What are the bases for the probabilites associated with the two human errors?

Page 2-6 - $B4S_{23}$ -€- What is the basis for the probability value associated with the operator error in switching to circulation too soon?

Page 2-6 - $B4S_6$ -€- What is the basis for the probability value associated with the operator failure to reconfigure valves for recirculation?

Page 2-8: Second paragraph, items (A) and (B) - Where is the EFS steam admission valve shown on Figure 2.1? If it is not indicated on Figure 2.1, how can the conclusions in these items be reached?

Page 2-9: Fourth paragraph - Who is supposed to perform the sensitivity analysis mentioned in this paragraph and on what schedule?

Page 2-13: Figure 2.1 - How can the loss of offsite power sequence be an initiator? Regarding T_{2A} T_{10}-δ, isn't Figure 2.1 independent of the containment failure mode?

Page 3-1: Second bullet - where are the findings about SHA effects found in WASH-1400? This statement appears to conflict with the statement on page I-8 of Appendix I to WASH-1400 regarding SHA effectiveness.

Page 3-1: Third bullet - What is the basis for the conclusion that the ECF event on the large LOCA tree in WASH-1400 was based on extremely conservative assumptions regarding lack of functionability?

Page 3-1: Fourth bullet - How do you reconcile this statement with item 3 on page 3-18? It appears that this report has done the same thing (namely assume that transient-induced LOCAs caused by failure of Primary System Pressure Relief result in core melt) that it criticizes WASH-1400 for doing. Also see comments regarding page 3-18.

Page 3-7: First paragraph - Transient occurrence frequencies calculated using the data in EPRI-NP-801 are questionable because of the method used to tabulate the data. The interpretation of the EPRI data base is a point of controversy in the review of ATWS. Therefore, any results obtained using the EPRI data, including event sequence probabilities (see Section 4 comments), may be suspect.

Page 3-10: Last line at bottom of page - rest of text following "Section" is missing.

Page 3-15: Items M & L - What is the basis for the 24 hour requirement?

Page 3-16: Item U - Why not use "HPI" instead of "charging"?

Page 3-17: Primary System Makeup - Why not use "HPI" instead of "makeup"?

Page 3-18: Item 3 - In the exception, what is the basis for the statement that, "the excess RCS pressure is not expected to be very great"? Also, failure of primary system pressure relief may result in a RCS rupture with core melt, which was treated in WASH-1400 on the transient event tree as a core melt.

Page 3-20: Items F, Z, & H - What is the basis for the 24 hour requirement?

Page 3-23: Footnote - What is the basis for the conclusion that ATWS sequences were considered relatively unlikely to have a significant impact on total risk?

Page 3-24: Figure 3.1 - Why aren't branches with failure of primary pressure relief function terminated as LOCA, since they lead to RCS rupture due to overpressurization?

Page 4-1: Section 4.0 - Shouldn't some additional explanation be included about why use of the WAMCUT computer code causes differences in the quantification techniques? What is different about WAMCUT as opposed to the codes used in the WASH-1400 work?

Page 4-2: First paragraph - By whom were the failure modes monitored? The NRC single failure criterion only addresses active failures. It does not include passive failures in its current form.

Page 4-2: Third paragraph - Did the quantification of operator errors distinquish between actions where the operator has experience (e.g., initiation of EFS) and those actions where he has less experience? How was the time which the operator has for action in mitigating the events considered accounted for in the quantification? Were stress levels considered?

Page 4-3: Second paragraph - What is the basis for a coupling coefficient of 0.1?

Page 4-7: Third paragraph - Is this the basis for the 24-hour requirement in preceding sections?

Page 4-8: Second and third paragraphs - This discussion appears to address several comments made previously about Section 4. Why doesn't it appear earlier in the section?

Page 4-10: Entire page - Isn't this material redundant to that in Section 3? Why repeat it here?

Page I-1: Volume 2, Part I, Bullets - There is no one-to-one correspondence between the bullet items and the major headings in Appendix I.

Page I-6: ECCS Recirculation Mode - In order to provide balance in Section I.4.1, the three system descriptions preceding this paragraph should be under the heading "injection mode."

Page I-7: Second paragraph - What does non-seismic mean?

Page I-8: Section I.6 - Denote Section number.

Volume 2, Part II

General comment on quantification of fault trees: It was extremely difficult and in some instances impossible, to follow the quantification of the fault trees for each system considered in the study. This was particularly true in cases where coupling was considered (e.g., Figure D.3 on page D-21). The relationship between the fault trees and the accompanying quantification tables and Boolean equations was not always clearly described. Since this treatment is a very important part of the report, it should be expanded or at least clarified so that the reader can verify the quantification of the fault trees without considerable difficulty.

We agree with H. Ornstein's comments regarding the assessment of human errors and operator errors. We also agree with his comment regarding the use of actual plant test and maintenance data and the use of lower bound failure rate data (e.g., ESAS relay failure rate data) as a computational median to obtain unavailabilities.

Page II-4 - Step 10, What is the basis for this assumption when there is ample evidence from LERs that tech specs are violated not infrequently?

Pages A-1 to A-28 - Appendix A - Based on the discussion between SAI and FPC on June 18, 1980, it is our understanding that this appendix will be revised to provide a reliability analysis of the RPS, not the control-grade anticipatory reactor trips. In the revision the following comments on Appendix A should be considered:

(1) Page A-9: Notes on CRD Power Train - First bullet - Is it possible to reset the CRD control panel without having reset the breaker? If so, was this considered in this study?

(2) Pages A-16, A-17: Figures A.3 (1/2 & 2/2) - How is the human error consisting of failure to reset the CRD breaker after testing included in the simplified RPS fault tree? Are there any common mode failures associated with the RPS?

(3) Page A-22: Figure A.4 (1/2) - Why does this figure differ from Figure A.3 (1/2)?

Page B-4: First paragraph - What does DGELS mean?

Page B-24: First paragraph - Is equipment miscalibration the only common-mode human error?

Page C-22: Second level on fault tree - What type of gate should this be?

Page C-24: Second level on fault tree, rightmost branch - Same comment as page C-22 above.

Page D-23: First level on tree - Shouldn't this be an "and" gate?

Page D-28: Under Top Events, shouldn't the term on the left side of the fifth Boolean equation be "MCC3AB"?

Page E-1: Third paragraph - Are there three pumps or five pumps in the NSCCCS?

Page E-20: Second paragraph - The contribution of simultaneous hardware faults in both NSCCS pump train is a factor of two smaller than what?

Page G-4: Second bullet - Identify the figure referred to.

Page G-7: First bullet - What is the basis for this statement?

Page P-2: First paragraph - Define the term "non-seismic".

Appendix P - General comment: How did the results of this study compare with the reliability analysis of the EFS performed by B&W and FPC?

Page P-24: First sentence - Why wasn't failure of all AC power considered in this study? This event is considered in the auxiliary feedwater system reliability study required of all PWR licensees through NRR's implementation of Action Item II.E.1.1 of the NRC's TMI-2 Action Plan.