UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

March 14, 1980

MEMORANDUM FOR: Harold R. Denton, Director
Office of Nuclear Reactor Regulation

Carl Michelson, Director
Office of Analysis and Evaluation of Operating Data

THRU: Robert J. Budnitz, Director
Office of Nuclear Regulatory Research

FROM: Robert M. Bernero, Director
Probabilistic Analysis Staff
Office of Nuclear Regulatory Research

Frank H. Rowsome, Deputy Director
Probabilistic Analysis Staff
Office of Nuclear Regulatory Research

SUBJECT: SINGLE FAILURE POTENTIALLY LEADING TO CORE DAMAGE

The purpose of this memo is to alert you to an alternate sequence of events for a two-year old incident that could easily have resulted in an outcome as serious as that of the accident at Three Mile Island. This newly-discovered close call is significant for the clues it provides for ways to improve regulatory requirements and incident evaluation. The specific accident vulnerability has already been rectified by bulletins and orders spawned by TMI and IE Bulletin 79-27.

A review of the incident at Rancho Seco on March 20, 1978 (the incident of the dropped light bulb leading to a de-energized bus, extensive instrument failures, and a severe over-cooling transient) by PAS indicates that the incident could have led to core damage had the incident taken a slightly different course. No additional failures would have been required for this outcome. It appears that the loss of the Non-Nuclear Instrument Bus NNI-Y had the following effects:

1. It caused a loss of main feedwater. (The Integrated Control System was operable but its input signals were faulted by the NNI-Y interruption, leading it to close the feedwater control valves.)

2. It could easily have defeated the autostart of the Auxiliary Feedwater System. (A faulted and randomly drifting steam generator level indication happened to drift low enough to start the AFWS several minutes into the transient--it might well not have done so.)

3. Instrument faults blinded the operators to the status of the secondary coolant system and to many primary coolant system parameters, e.g., loop temperatures.

For more details of the historical event, see, e.g., the memo of Richard Lobel to Paul Check, "Summary of Meeting Held at Rancho Seco Nuclear Power Plant on July 10, 1978 to Discuss a Recent Cooldown Event," July 31, 1978.

Had the Auxiliary Feedwater System not delivered flow, as it did after the coincidental autostart signal occurred, the steam generators would have remained dry. The primary coolant system would have remained without a heat sink. Decay heat would have boiled the reactor coolant, with relief via the pressurizer safety valves (the PORV was gagged closed). The two instruments that the operators trusted, according to subsequent accounts, would have indicated slightly higher-than-normal reactor coolant system pressure and high pressurizer level.

Under these circumstances it is quite plausible that the operators would have failed to recognize the need to start feedwater flow manually to achieve steam generator cooling or alternatively to start HPI manually to achieve feed-and-bleed cooling. Thus, the boiloff of reactor coolant might have continued unrecognized until containment high pressure or high radiation ESFAS setpoints were reached. These would have autostarted HPI and the AFWS, but not necessarily before core damage had been done.

We are less concerned about the current safety of Rancho Seco--which appears to be acceptable-than we are about the broader implications that such a vulnerability to a single-failure-induced core damage scenario could have escaped detection in the licensing and incident review processes.

Our confidence in the comparative safety of Rancho Seco with respect to this scenario is based on the following considerations. Having once experienced and analyzed a loss of power on NNI-Y, the operators at the plant presumably can recognize the symptoms, have some insight into the consequences, and know the ways to restore power should it happen again. The accident at TMI has engraved upon the minds of PWR operators that a very high pressurizer level is not, by itself, cause for reassurance about core cooling. The bulletins, orders, and NRC-mandated operator training make it very unlikely that the operators would trust feedwater delivery without instrumental verification or would be lulled into complacency by a very high pressurizer level under upset conditions. Under these circumstances we think it very unlikely that another power outage on NNI-Y at Rancho Seco would result in core damage today, although it might well have done so in 1978.

The permanent fix for this class of accident sequences appears to have been covered by the bulletins and orders. That is, the study of instrument power supply faults required in IE Bulletin 79-27, the installation of a safety-grade autostart for the Auxiliary Feedwater System and the addition of control room instrumentation specifically dedicated to the assessment of the adequacy of core cooling will resolve this class of vulnerabilities. A key point should be emphasized in the design bases for these modifications: these add-ons should be free of common-cause failure modes linking the failure of the add-on to the failure of the Main Feedwater System, the ICS, or the other normal control and support systems. We understand that SMUD has committed to the installation of the safety-grade actuation system for the Auxiliary Feedwater System by January of 1981, and has already rearranged the power supplies for some key instruments so that no one failure disables so much instrumentation.

There have been several other instances in which a non-safety grade instrument power supply failure has caused the ICS of a B&W plant to misbehave. Two of these were at Crystal River Unit 3: one on March 2, 1977 and another on February 26, 1980. Others have occurred at Oconee, e.g., the event at Oconee Unit 3 of November 10, 1979 which spawned IE Bulletin No. 79-27. These events appear to be of two kinds. In one kind, exemplified by the Rancho Seco and most recent Crystal River events, the power supplies for the ICS remain energized and the ICS functional. However, many of the input signals upon which the ICS and the operators depend are faulted, leading to rather schizophrenic behavior by the ICS. In the other kind of event, one of the ICS power supplies fails, causing several of the ICS-controlled devices to shift to their "failed" state. No single analysis of a particular bus fault and its expected consequences covers all the possibilities.

A quick review of the sequence of events for the recent Crystal River incident suggests the following safety problems associated with the ICS or Rupture Matrix response, which might become important in alternate sequences of events:

1. The ICS withdrew the rods and shut off main feedwater in response to the spurious indication of low Tave. This would have amplified the severity of an ATWS event. The ICS terminated rod withdrawal at 103 percent power so the rod withdrawal effect on ATWS severity would have been small. We see no reason to suspect a common cause failure to scram, but without a careful search for common cause mechanisms we cannot be sure. It should be noted that random failure to scram may not be as improbable as we would like to think. The LERs contain instances of the discovery of possible ground faults in the scram logic of B&W plants which were not detected by routine surveillance tests, and which were not "fail safe." (Refer to LER Accession No. 138211, Event Date 5/9/78, Crystal River Unit 3.)

2. The ICS shut off all feedwater delivery to the steam generators without terminating all steam demands on the steam generators. This appears to have happened only briefly to both steam generators at CR-3; this condition persisted in the Rancho Seco incident. Since B&W steam generators boil dry very rapidly, even when bottled up, the continuance of steam flow can rapidly deplete the steam available for turbine driven emergency feedwater pump(s). We have identified two mechanisms for this steam bleed: in both the Rancho Seco and recent Crystal River incidents, the turbine driven main feedwater pumps apparently remained running after the main and startup feedwater control valves closed. This is useful in stretching the time window within which main feedwater flow can be resumed; but after steam generator dryout, it runs the risk of defeating the backup turbine driven emergency feedwater pump(s) as well. The other mechanism lies in the possibility that a faulted ICS might command open the power operated main steam atmospheric dump or other steam valves. This could seriously compromise safety in a plant having only turbine driven and no motor driven emergency feedwater pumps, e.g., Davis Besse or Oconee. This latter failure mechanism has not been observed, to our knowledge. Further study is necessary to determine whether this is a real problem at any of the B&W plants.

3. The protection system for main steam line breaks, called the Rupture Matrix at Rancho Seco, is actuated when the steam generator pressure falls to 600 psi. This low pressure can be caused by over-cooling by emergency feedwater or by the steam bleed problems noted above. It results in cutting off all feedwater and tripping the main steam isolation valves. This is a poor way to correct automatically for excessive emergency feedwater flow as it requires operator intervention to override the protective function to restore emergency feedwater. Steam pressure to restart the turbine driven emergency feedwater pump might not be available by the time the operators recognize the need. At Davis Besse there is an interlock to prevent the main steam line break isolation system from isolating both steam generators, but there appears to be no such interlock at Rancho Seco. It should be noted that the Rupture Matrix is effective in limiting the steam bleedoff caused by the continued operation of the turbine-driven main feedwater pump(s). It is not clear whether or not it would override a spurious "open" command to the atmospheric steam dump valves. As a result, the Rupture Matrix may be a useful as well as a potentially counter-productive feature in these control fault scenarios.

In many respects IE Bulletin No. 79-27 addresses these problems in the short term. It calls for studies of the effect of Class 1-E and non- 1-E instrument power supplies on the ability to achieve cold shutdown and requires the development of emergency procedures to deal with bus faults. It could be improved, in our estimation, by giving priority to the study of sequences in which successful core cooling may be in question, and by a focus on the kind of thorough scenario analysis necessary to fully explore the range of fault-effects, such as those noted above, that might be missed in a study aimed at problems in the way of achieving cold shutdown.

The observations on the recent incident at Crystal River Unit 3 should be regarded as preliminary and tentative. We shall follow this memorandum with recommendations on approaches to safety analysis that can give greater confidence that vulnerabilities such as the one exemplified by the Rancho Seco alternate sequence are detected and evaluated.

FHR for RMB

Robert M. Bernero, Director
Probabilistic Analysis Staff
Office of Nuclear Regulatory Research

Frank Rowsome

Frank H. Rowsome, Deputy Director
Probabilistic Analysis Staff
Office of Nuclear Regulatory Research

cc: P. Baranowsky, PAS
M. Cunningham, PAS
J. Curry, PAS
G. Edison, PAS
D. Eisenhut, NRR
N. Haller, MPA
S. Hanauer, NRR
R. Mattson, NRR
T. Murley, RES
J. Murphy, PAS
K. Murphy, PAS
T. Novac, NRR
D. Ross, NRR
M. Taylor, PAS
D. Vassallo, NRR
W. Vesely, PAS