REFERENCE 3

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

April 21, 1981

NOTE TO: Gus Lainas

FROM: Ashok Thadani

SUBJECT: FREQUENCY OF EXCESSIVE COOLDOWN EVENTS CHALLENGING VESSEL INTEGRITY

REF. 1: Memorandum from M. Taylor to S. Fabic dated October 29, 1980

In response to your request of last Friday, April 17, the enclosure provides a very preliminary (weekend effort) assessment of the likelihood of a severe overcooling event which could challenge the pressure vessel integrity. Although our quick assessment suggests that the likelihood of overcooling events such as the one that occurred at Rancho Seco is lower (than that estimated in Reference 1) due to the assumed hardware modifications implemented at the B&W plants (this assumption should be verified by DL), there is considerable uncertainty in the hardware and human error rates assumed in this hasty analysis. This assessment suggests that the likelihood of severe overcooling events is not so high as to require precipitous action, but I strongly urge you to consider the preliminary nature of this analysis and initiate a program to more systematically estimate the likelihood of severe overcooling events.

Ashok C. Thadani, Acting Chief
Reliability & Risk Assessment Branch
Division of Safety Technology

Enclosure:
Preliminary Assessment

cc: T. Murley
M. Ernst
R. Bernero
M. Taylor

8105110215

Preliminary Assessment of the Frequency of Excessive Cooldown Events Challenging Vessel Integrity

Excessive cooldown events in PWRs can occur in a variety of ways--leak/break in the primary system, leak/break in the secondary system, and excess feedwater flow. Of concern are those events that could challenge the pressure vessel integrity by cooling the plant down to about 250°F while achieving primary system pressures above roughly 1000-1500 psi. Protection against challenging the pressure vessel integrity for these types of events (which are not terminated by automatic isolation of the steam generator) is dependent on operator action. These actions are initiated by the pressure-temperature limit curves in the Technical Specificiations. However, the emergency operating procedures are generally not explicit in treating pressure vessel integrity.

Following initiation of a severe depressurization event, the operator would assure that core cooling systems were functioning such as ECCS and feedwater to the steam generators. These actions could lead to continued cooldown and repressurization of the primary system. Subsequently, the operator would try to terminate the source of the depressurization by closing the PORV block valves or isolating the steam generators as conditions indicate. This action would stop the cooldown and, if performed soon enough, would preclude challenging the pressure vessel integrity. If severe pressure vessel cooling is not stopped in time, the operator must control the primary system pressure by terminating HPSI, using pressurizer sprays, increasing letdown flow, or opening the PORV. These actions are complicated by:

1. No procedures indicating best approach for controlling a highly dynamic situation.

2. Mind set after TMI-2 accident to keep HPSI operating.

3. Normal pressurizer spray is unavailable because RCPs are tripped following an SIS.

4. Auxiliary pressurizer spray may not be available because of interlocks with SIS.

5. PORV controls may not be convenient and the rapid pressure response would tend to result in see-saw control.

6. Repressurization may be very rapid depending on the transient dynamics.

The time available for operator action depends on the plant status prior to the event. If the plant is at power (>30%), the decay heat will delay the pressure vessel cooldown to critical temperatures by a factor of about 2, compared to the low decay heat condition (hot standby). However, it is assumed that hot standby conditions occur only about 5% to 10% of the operating time.

Rough estimates were made of the initiating frequencies for various events. Only small LOCAs need be considered because large LOCAs will preclude repressurizing the primary system. Small-small LOCAs (<2-inch) which have a frequency of about 10^{-2} - 10^{-3}/RY will either depressurize very slowly or repressurize with full ECCS operational. The primary system temperature will be held up by heat removal through the steam generators unless the steam generator isolation fails (assumed unavailability <10^{-3}/D). Thus, a small-small LOCA is not considered a major contributor to pressure vessel challenge. A small LOCA (2-inch and up) has an estimated frequency of 3 x 10^{-4}/RY (WASH-1400) and could result in a challenge to the pressure vessel integrity sometime during the depressurization transient depending on the relative rates of cooldown and primary system depressurization. The small LOCAs of interest are assumed to be relatively slow events (>1 hour) which would permit operator action.

Large steam/feedwater line breaks have an estimated frequency of 10^{-4}/RY based on Ref. 1. These events are potentially capable of achieving critical vessel temperatures depending on isolation of the steam generator (both inlet and outlet lines) and its initial water inventory. B&W plants have a very small S.G. inventory which may preclude achieving critical vessel temperatures if feedwater is not added to the faulted steam generator. The large steam/feedwater line breaks that ultimately get to critical vessel temperatures are assumed to be moderately fast (~30 minutes).

Small steam/feedwater line breaks, including unisolated stuck-open relief valves, have an assumed frequency of 10^{-2} - 10^{-3}/RY (similar to LOCAs) and their response should be relatively slow (~1 hour to get to critical vessel temperatures). The availability of block valves for the steam generator relief valves and instrumentation indicating a stuck-open relief valve is uncertain. Therefore, a conditional probability of 0.1/D was assumed for isolating a stuck-open relief valve.

Transients initiated by failure of the feedwater control system could result in severe overcooling events as shown by the Rancho Seco incident of March 1978. The critical characteristic of this event is that adequate control room readout of steam generator conditions and primary system was lost for over an hour which precluded the operator from taking appropriate action. We believe that if adequate primary system and steam generator information are available to the operator in the control room, the operator failure to terminate a severe overcooling event, caused by feedwater controller failure, is significantly reduced. The sequence of interest is a common cause failure like loss of instrument and control power which initiates the transient and "blinds" the operator.

Prior to the Rancho Seco event, in B&W plants, one of the NNI buses supplied power to the integrated control system (ICS), which controls feedwater (main and auxiliary) and steam generator pressure control, and to certain vital primary system and steam generator instruments. As a result, the loss of this one bus could initiate severe transients and hamper the operator response. According to Ref. 2, there have been 29 NNI/ICS power failures in about 28 reactor-years of operation which yields an estimate of the failure rate of 1/RY. Since power was not restored for over an hour in the Rancho Seco event, the point estimate for the conditional probability of not restoring power in 1 hour <u>and</u> having a significant transient is 1/29 or 0.033/D. This estimate may have a large uncertainty. Thus, the observed frequency for severe overcooling transients which might challenge the pressure vessel integrity was 0.03/RY for the B&W designed plants prior to the assumed implementation of the instrument channel modifications discussed below.

After the Crystal River event of February 1980, the staff recommended that at least two redundant channels of vital instrumentation be provided in the control room (Ref. 2). Implementation of this recommendation would preclude ICS failure and loss of instrumentation when one NNI/ICS bus fails. There is a possibility of common cause failure of two control and instrumentation power buses. A review of LERs on inverter failures in Ref. 3 indicated that there have been four situations when two inverters were lost out of 140 inverter failures. This yields a crude estimate of the conditional failure of a second inverter given the loss of one inverter of 0.03/D. Using these estimates and assuming two separate instrument channels yields an estimated frequency of 10^{-3}/RY for severe overcooling transients which might challenge the pressure vessel integrity.

It is our understanding that Westinghouse and Combustion Engineering plants have a power supply for the feedwater control or separate from at least two vital instrument power supplies. This power supply separation coupled with the thermal inertia in Westinghouse and CE plants should result in a much lower probability of severe overcooling transients.

The probability of the operator successfully controlling a severe overcooling event depends on several factors--training, rapidity of the transient, ability to terminate cooldown, capability of controlling primary system pressure, available instrumentation, mind set, etc. The following crude estimates of human error probabilities (HEP) were made on the assumption that the operator is trained to stay within the pressure-temperature limits <u>and</u> maintain adequate primary system subcooling.

1. Able to terminate subcooling transient, instrumentation is available, and transient takes more than 30 minutes.

   The HEP is assumed to be 3×10^{-3}/D based on WASH-1400 analysis of switchover from injection to recirculation. This action is considered to be equivalent since the operator would be trained to isolate faulted steam generator, etc.

2. Control of primary system pressure after pressure vessel cooled down to critical temperatures, instrumentation available, and transient takes more than 30 minutes.

   The HEP is assumed to be 3×10^{-2}/D since this action requires dynamic control on the part of the operator which is more complicated than item 1 above.

3. Control of primary system pressure after pressure vessel cooled down to critical temperature, instrumentation available, and a time frame less than 30 minutes.

The HEP is assumed to be 0.3/D based on a high stress situation and human error evaluations presented in Ref. 4.

4. Inadequate instrumentation to monitor transients and over 30 minutes to respond.

   The HEP is assumed to be 0.6/D assuming the operator is trained to monitor pressure-temperature limits.

A summary of the estimated probabilities for sequences that might challenge the pressure vessel integrity is presented in Table 1. There is an uncertainty of 2 to 10 in the HEPs and an uncertainty of a factor of 3 in the initiating frequencies. The probability of having a critical flaw size in the pressure vessel has not been included in these assessments. Similarly, other sequences involving single failures of components which might inhibit operator action or automatic features that would limit the event have not been developed.

	Initiation Frequency	Operator HEP	Sequence Probabilities
LOCA (>2")	3×10^{-4}/RY	3×10^{-2}/D	10^{-5}/RY
Large steam/feedwater line break	10^{-4}/RY	3×10^{-2}/D	3×10^{-6}/RY
Small steam/feedwater line break	10^{-2} - 10^{-3}/RY	3×10^{-2}/D	3×10^{-5}-3×10^{-4}/RY
Severe Overcooling transient caused by loss of control/ instrument power			
B&W (one-bus design)	3×10^{-2}/RY	0.6	2×10^{-2}/RY
B&W (two-bus design)	3×10^{-2}/RY	3×10^{-3}/D	9×10^{-5}/RY
	10^{-3}/RY	0.6	6×10^{-4}/RY
W. & CE (three-bus design)	Expected to have lower probability of severe overcooling transients because of design differences compared to B&W.		

TABLE 1.--SEQUENCE PROBABILITIES

References

1. Memorandum from M. Taylor to S. Fabic dated October 29, 1980.

2. Transient Response of Babcock and Wilcox-Designed Reactors, NUREG-0667, May 1980.

3. Memorandum from J. Knight to F. Mensam undated (Inverter Failures).

4. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, October 1980.