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

OFFICE OF THE
COMMISSIONER

July 21, 1982

MEMORANDUM FOR THE CHAIRMAN AND COMMISSIONERS

SUBJECT: SAN ONOFRE UNITS 2 AND 3 ISSUE:) PORV

The San Onofre plants do not have power ope ated relief valves on the pressurizer. This means two ings:

First, there is no way to depressurize the primary system quickly during a steam generator tube rupture. Depressurizing the primary system is necessary to stop the flow of contaminated water from the primary system to the steam generator and eventually to the environment. You will recall that the operators at Ginna used the PORV in just this way to stop the flow of radioactive primary coolant to the environment.

Second, if for one reason or another the steam generators are not available to remove heat, there is no way to depressurize the primary system to let ECCS water in. The discharge pressure of the ECCS pumps is lower than the setpoint of the primary safety relief valves, therefore cooling the core by the "feed and bleed" mode is impossible. This method was of course the principle decay heat removal path at TMI while the primary system was bound with steam and hydrogen.

This issue also comes up for the Combustion Engineering reactors in the Palo Verde units. On my visit there, utility officials told me they intend to provide PORV's.

Southern California Edison has taken a different tack. It is emphasizing the reliability of its steam generators and auxiliary feedwater system. A recent Southern California Edison letter to the NRC staff seeks to postpone the decision on adding PORV's until the Combustion Engineering Owners Group completes its deliberations on the subject. The date for completion of those deliberations is not stated. Meanwhile the Commission must vote on a full power license for Unit 2.

50-361 & 362

I think the arguments for a depressurization capability are clear. I would not insist on it for startup of the San Onofre units, but I would attach a license condition requiring installation of a PORV within a reasonable period of time, say by the first refueling.

EA for
Victor Gilinsky

cc: SECY
OPE
OGC

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

(8)

JAN 29 1982

MEMORANDUM FOR: Bob Tedesco, Assistant Director for Licensing
Division of Licensing, NRR

Themis Speis, Assistant Director for Reactor Safety
Division of Systems Integration, NRR

FROM: Frank H. Rowsome, Deputy Director
Division of Risk Analysis, RES

Joseph A. Murphy
Reactor Risk Branch
Division of Risk Analysis, RES

SUBJECT: FEED AND BLEED ISSUE FOR CE APPLICANTS

We have performed a quick and dirty analysis of the risk implications of CE designs that lack a capability for core cooling via HPI injection and deliberate venting of the reactor coolant system, in the absence of feedwater replenishment.

We conclude that three classes of accidents may each be more frequent than the Commission's safety goal of 10^{-4} core melts per reactor year or less, and that the total core melt frequency for such plants could be of the order of 10^{-3} per year or more. The three sequences are:

1. Transient and failure of all feedwater (not associated with loss of AC power) (TML).

2. Loss of offsite power, one diesel failure disabling the motor driven AFW train, and failure of the turbine-driven AFW train.

3. Very small LOCA and failure of HPI (S_2D).

STEVE HANAUER

* COMBUSTION ENGINEERING PLANTS

ROWSOME SAYS SEP ($10^{-4} \approx 10^{-5}$) MAY BE INADEQUATE

5.

50-470
Dupe of
8202220394 XA

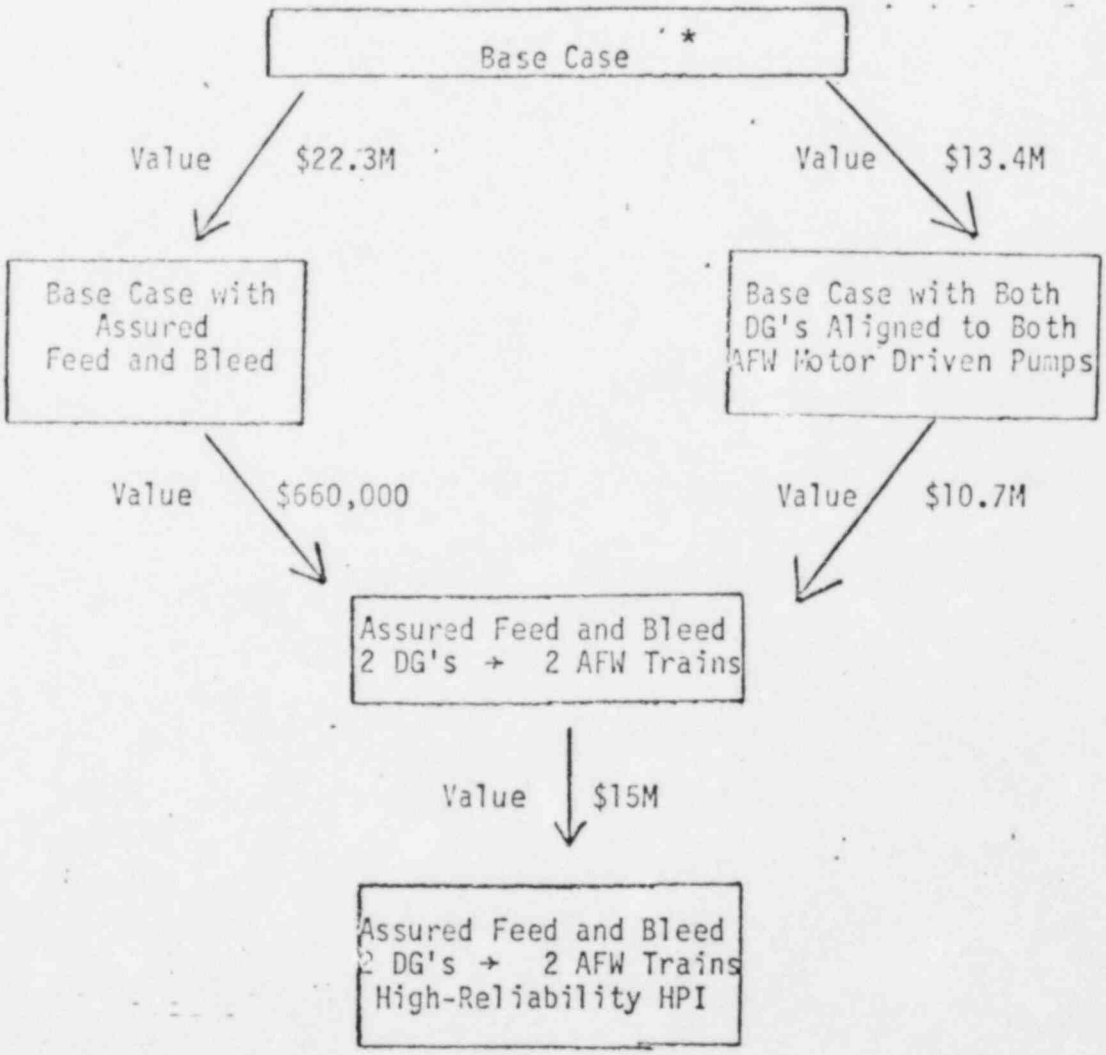
We recommend the following upgrades to these designs:

1. Provide an assured "feed and bleed" capability.

2. Provide that either diesel generator can energize a motor driven AFW train.

3. Examine carefully and perhaps upgrade HPI reliability and/or reduce the frequency of very small LOCA's.

The economic incentives to make these improvements, derived from reduced risk of economic losses associated with core melts, are roughly:



*The base case plant is assumed to be incapable of feed and bleed cooling, only one diesel generator is assumed capable of energizing the safety related motor driven AFW train. The turbine driven AFW train is AC-independent, but the non-safety grade motor-driven AFW train requires offsite power. Industry average HPI reliability and S_2-LOCA frequency is assumed. The analysis that shows that S_2D may be too frequent applies to other PWRs as well.

The attached paper describes the analysis.

Frank H. Rowsome, Deputy Director
Division of Risk Analysis
Office of Nuclear Regulatory Research

Joseph A. Murphy
Reactor Risk Branch
Division of Risk Analysis
Office of Nuclear Regulatory Research

Attachment: As Stated

cc: R. Bernero
G. Burdick
R. Mattson
S. Hanauer
M. Ernst
A. Thadani
RRB Staff
RAB Staff

We understand that the current crop of CE license applicants are proposing that no pressurizer PORV's be installed, that the HPI shutoff head is to be well below the pressurizer safety valve setpoint (around 1400 psi), that high point vents provide no more than two 1" diameter remote-manual vents, and that the auxiliary feedwater systems will be composed of one AC-independent turbine driven pump, one AC-power train, and a third non-safety grade motor driven pump.

We have attempted a back-of-the-envelope PRA in order to evaluate the risk implications if these plants are incapable of "feed and bleed" cooling. The results suggest that they may fail to meet the Commission's safety goal of a core melt frequency less than 10^{-4}/year and the present worth of a fix to enable assured feed and bleed cooling is of the order of $10 million or more per plant, based upon reduced financial risk alone. We considered five groups of accident sequences: loss of main feedwater, loss of offsite power, very small LOCA, transient-induced small LOCA (late start of auxiliary feedwater allows a lift of a pressurizer code safety valve which may stick open), and station blackout with restoration of AC power just before the point-of-no-return. We did not consider main steam line breaks or ATWS, although in these sequences an assured feed and bleed capability could also enhance safety as well as in the sequences considered.

The simple loss of main feedwater appears to be the dominant concern. For this sequence in a plant incapable of feed and bleed cooling, the frequency of core melt, $\lambda_{cm} = \lambda_m P(L)$, where λ_m is the frequency of critical (sustained) failures of main feedwater, and $P(L)$ is the probability of a critical failure of the auxiliary feedwater system.

WASH-1400 took the frequency of feedwater transients to be 3 per year, with 99 out of one hundred such occurrences recoverable. There is reason to doubt both numbers. Complete interruptions of main feedwater are more frequent than 3 per year during the life of the first core, while the plant is still being debugged, although many take place at startup or at low power when the decay heat level is too low to pose much risk. A mature plant has complete interruptions of main feedwater about once a year or less. The non-recovery factor of 10^{-2} applies to plants with simple feedwater controls, motor driven main feedwater pumps, and no major obstacles to feedwater restart after a trip. In large, modern plants with turbine-driven main feedwater pumps problems with feedwater restart are common, so a non-recovery factor of .3 to .1 is more reasonable. I judge that the frequency of non-restorable failures of main feedwater occurring from substantial (risky) initial power levels is roughly:

$$\lambda_m = \begin{cases} 0.3 \times 10^{\pm 1}, & \text{first core} \\ 0.1 \times 10^{\pm 1}, & \text{at maturity} \end{cases}$$

Auxiliary feedwater reliability is also uncertain. Data from the precursor program suggests that the PWR average experience has been a failure probability of 10^{-3}/demand. This average includes early-in-life experience as well as mature plant experience and two train as well as three train experience. System reliability analyses have suggested that the best of the three train systems can approach - at maturity - 10^{-5} per demand. However, these analyses failed to consider some common mode failure mechanisms so they can be regarded as having an optimistic bias. It is not uncommon early in plant life to find instances of repeated, consistent, auxiliary feedwater pump failures while the system is being debugged in service. The record suggests that the failure probability of the AFWS is substantially higher during the first core than in maturity. A system with two diverse safety grade AFW trains and a third full capacity non-safety grade train will probably achieve failure probabilities of:

$$P(L) = \begin{cases} 3 \times 10^{-3\pm1}, \text{ first core} \\ 1 \times 10^{-4\pm1}, \text{ at maturity} \end{cases}$$

These estimates result in loss-of-all-feedwater frequencies of:

$$\lambda_{cm} = \begin{cases} 0.9 \times 10^{-3\pm1.4}/\text{yr}, \text{ first core} \\ 1 \times 10^{-5\pm1.4}/\text{yr}, \text{ at maturity} \end{cases}$$

The uncertainty range is thus:

$$2.3 \times 10^{-2} \gtrsim \lambda_{cm} \gtrsim 3.5 \times 10^{-5}, \text{ first core}$$
$$2.6 \times 10^{-4} \gtrsim \lambda_{cm} \gtrsim 3.9 \times 10^{-7}, \text{ at maturity}$$

Note that even at maturity this core melt sequence frequency may be higher than the Commission's criterion for all core melt frequencies combined: $\lambda_{cm} \lesssim 10^{-4}$/yr, and that the best estimate is that it will exceed the Commission's criterion during the first core. Note also that common-causation of main and auxiliary feedwater failure due to fires, floods, earthquakes, or sabotage has not been considered and might increase this sequence frequency. The Commission's guidelines on acceptable risk do not indicate how to treat uncertainties or higher-than-average estimates for the first core. Nonetheless, I think it unwise to allow a single core melt accident sequence to be this probable. The provision of an assured feed and bleed capability would enable HPI to cool the core in these scenarios. Even with common mode and external hazards, this should be worth at least one decade, more likely two decades reduction. We recommend it.

Next let us consider loss of offsite power. The failure frequencies or probabilities are taken to be:

$\lambda_{LOSP} = 0.2$/yr

P non-recovery of offsite power within 30 min - 1 hr = 0.2/occurrence

Thus λ_{LOSP} without recovery = 0.04/yr

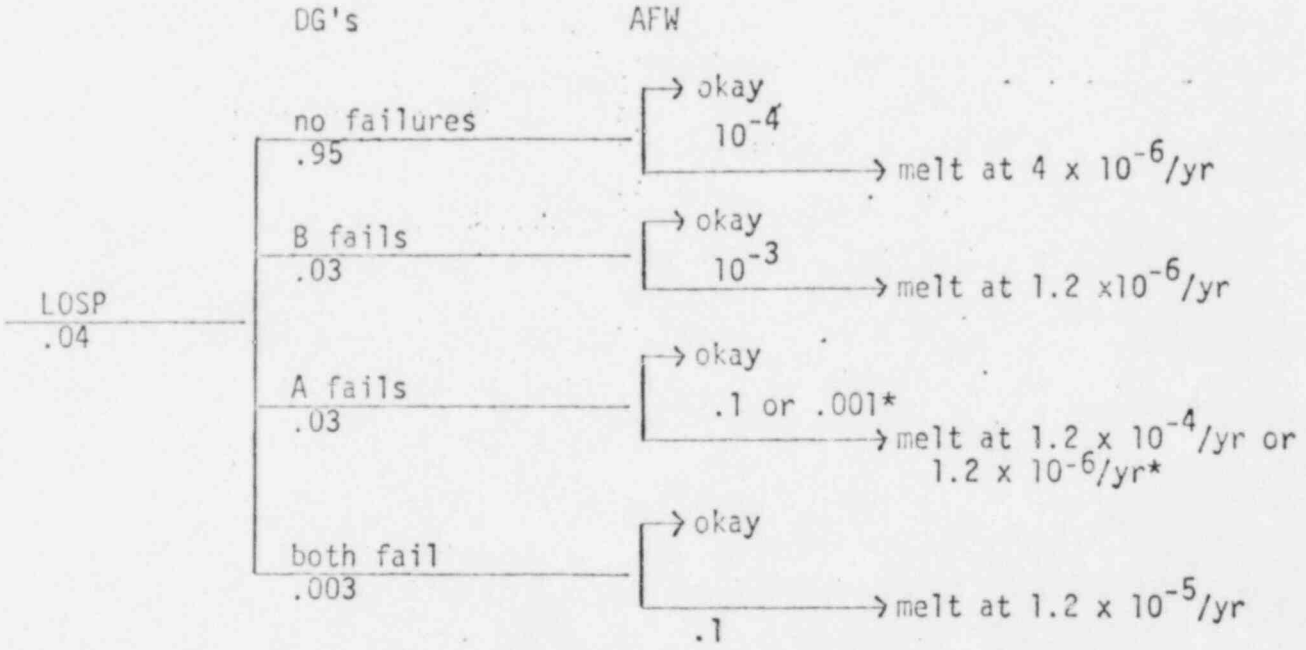
$P_{DG} = 0.03$/demand

$P_{2DG} = 0.003$/demand, including common mode

$P_{AFW\text{-}turbine\ train} = 0.1$/demand

$P_{AFW\text{-}motor\ train} = 0.01$/demand

Assume for convenience that diesel generator A is configured to energize the safety grade AFW motor driven train. As we shall see, the core melt frequency predictions are sensitive to whether or not diesel generator B can energize the non-safety grade AFW train or not. The event tree for loss of offsite power can be drawn:



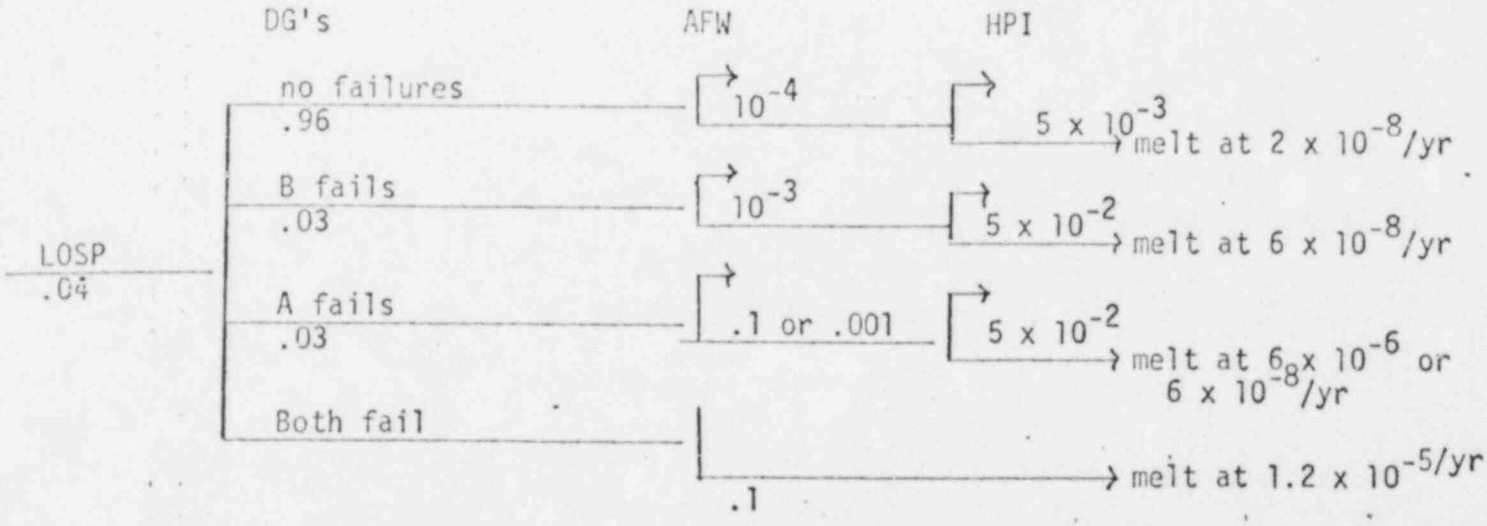
*The higher failure rate applies if one of the diesel generators (we have called it B) cannot power a motor driven AFW train; the lower failure rate applies if both diesel generators can power a motor driven AFW train.

Note that the Commission safety goal of 10^{-4}/yr for all core melt sequences may be violated by loss of offsite power and a single diesel generator failure if there is one diesel generator that cannot be aligned to energize a motor-driven AFW train. This high core melt frequency could be reduced to marginally acceptable value in either of two ways:

1. Insure that either diesel generator can be aligned to energize a motor-driven AFW train by (i) providing a swing bus for the safety grade AFW pump, or (ii) providing an essential (diesel-backed) power supply to the "non safety grade" AFW pump, or

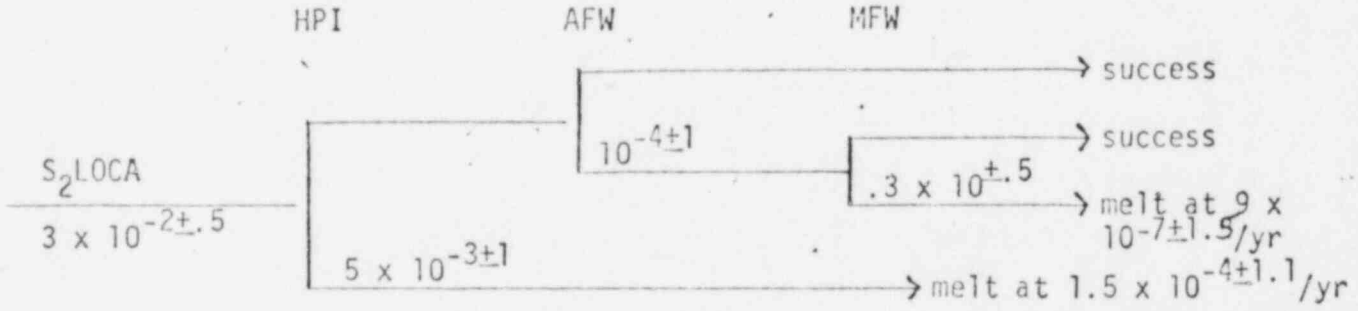
2. Provide an assured feed and bleed capability so that the one operable diesel generator and its associated HPI train can cool the core.

The case of full station blackout is considered later. The value of the feed-and-bleed fix can be inferred from the event tree for LOSP with this design:



Next let us consider very small (S_2) LOCA. Instrument line breaks, steam generator tube ruptures, charging pump line breaks, and gross reactor coolant pump seal failures have happened a dozen or so times in 500 LWR-years, suggesting a challenge frequency of $3 \times 10^{-2 \pm .5}$/yr for S_2LOCA excluding PORV LOCAs. They are less probable in the first year of service, so I will not single out first core numbers.

In the CE plants, both feedwater and ECCS (HPI) are required for successful core cooling. Main feedwater may remain operable or be restartable in some of these. The probability of HPI failure on demand was found to be $8.6 \times 10^{-3\pm.5}$ in Surry (WASH-1400). Most PWR PRAs are finding a failure probability for the whole multi-train HPI between 10^{-2} and 10^{-3}/demand. We shall assume that the probability of HPI failure on demand is $5 \times 10^{-3\pm1}$/demand for the CE plants. A rough cut at frequency estimation suggests:



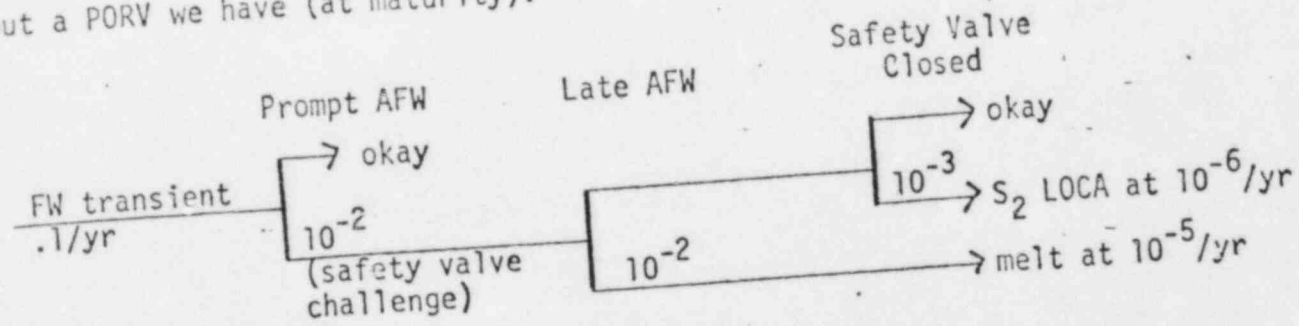
The value of an assured feed and bleed capability here is to eliminate the need for feedwater. This would eliminate the smaller (10^{-6}/yr) path to core melt without affecting the more prominent path via HPI failure. Note that small LOCA with total HPI failure is predicted to result in a core melt frequency above the Commission goal for all core melts. The provision of feed and bleed capability or of an improved AFW system will not help this. It is a problem generic to PWRs and not unique to the CE designs. It appears that the high frequency of very small LOCA revealed by historical experience and the marginal HPI system reliabilities revealed by many PWR PRAs are combining to yield unacceptable core melt frequencies through S_2D-type sequences. We suggest that NRR tackle this

problem in two ways: First, a serious effort should be made to reduce the frequency of S_2 LOCA's. Second, a broad-scale attack on HPI reliability problems comparable to that instituted for AFW systems after TMI should be initiated for all PWR's.

Next let us consider the transient-induced small LOCA's, with and without a PORV. A feedwater transient with a prompt autostart of auxiliary feedwater is assumed not to lift a pressurizer relief valve. However, a delayed start of AFW, which may be roughly one hundred times as likely as a sustained AFW failure, may lift a pressurizer valve (PORV or code safety) and the valve may stick open.

LER data suggest that PORV's stick open roughly once in one hundred challenges and code safety valves once in a thousand challenges. Neither type of valve have failed open spontaneously, to my knowledge, although there was one instance (Crystal River NNI bus fault) of a command fault leading to an open PORV. Since TMI I think it safe to assume that operators would successfully close the PORV block valve in at least 99 out of 100 instances of a PORV-LOCA.

Without a PORV we have (at maturity):



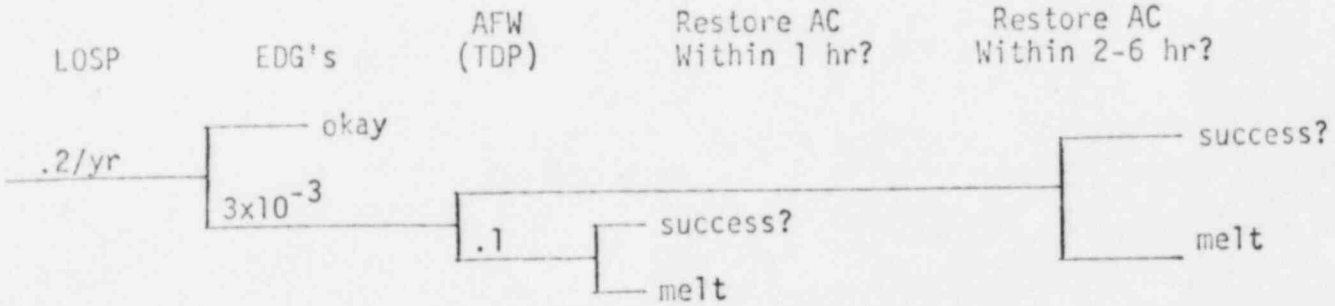
The core melt outcome from loss of all feedwater has already been considered. The increment in the likelihood of S_2 LOCA is negligible at 10^{-6}/yr. It can still be mitigated by HPI, if HPI works, as it will do in the vast majority of cases.

With a PORV we will get transient-induced LOCA ten times as often (10^{-5}/yr) but the block valve can be expected to terminate all but 1 percent of these for a frequency of transient-induced and unisolated LOCA of 10^{-7}/yr. If anything, the PORV helps rather than aggravates what is a negligible contributor to the overall S_2 frequency via transient-induced LOCA.

We should also consider the command fault LOCA's due to spurious "open" commands to a PORV. The frequency of occurrence is a sensitive function of the valve control logic design. It could be made as small as we wish by suitable reliability engineering. If we consider the Crystal River experience as one failure in 300 PWR-years, we get an industry average of 3×10^{-3}/yr for PORV command fault LOCA. Clearly, B&W did not do so well, but the combined experience of the three PWR vendors suggests that this frequency can easily be made much less than the overall S_2 frequency of $3\times10^{-2\pm.5}$/yr. I conclude that having a PORV or not having a PORV has a negligible effect on the likelihood of S_2 LOCA or of the likelihood that S_2 LOCA may lead to core melt, provided that system or component functional reliability is the only consideration. It goes without saying that this analysis is predicated upon a design with anticipatory trips so that routine transients do not lift pressurizer relief valves, and that the operators are trained to close the PORV block valve when appropriate.

There may also be a design adequacy issue. I feel uncomfortable with 1400 psi HPI pumps in plants without PORV's, even if the HPI and the AFW systems are highly reliable. Careful thermal hydraulic analyses together with thorough studies of plausible operator responses are necessary to verify that some S_2 LOCA's will not lead to degraded steam generator heat transfer and RCS pressures over 1400 psi while the core uncovers, even with operable HPI and AFW trains. The high point vents and reactor coolant pumps may help here even though these plants do not have full feed and bleed capability. However, these design adequacy issues are beyond the capability of this simplistic system reliability analysis.

Last, consider station blackout with AC recovery near the point of no return. The event tree may be drawn as follows:



Blackout with successful auxiliary feedwater (turbine driven pump) can be expected at a frequency of roughly 6×10^{-4}/yr. The turbine driven AF pump has a finite success window, however. One of several factors will lead to core melt if AC power is not ultimately restored. These factors include: (a) loss of reactor coolant inventory (blown RCP seals, etc.); (b) dead batteries (discharge or overheat); (c) high pump room temperatures (no HVAC); or (d) depletion of condensate.

Blackout without auxiliary feedwater leads to a shorter time window to save the core by AC recovery. This can be expected at a frequency of roughly 6×10^{-5}/yr. In either scenario, as the time to the point-of-no-return for core cooling approaches, the reactor coolant system pressure will be high, (around the pressurizer safety valve set point), and the level will be falling toward the top of the active core. Refilling the steam generators will be necessary but may not be sufficient, depending upon the effectiveness of reflux condensation and the extent of reactor coolant system leakage. A feed and bleed capability to enable HPI to refill the reactor coolant system fairly quickly might extend the window for AC recovery without core damage or melt by tens of minutes, perhaps more. A quantitative evaluation of the fraction of melt sequences that could be saved by feed and bleed would require extensive thermal hydraulic analysis and analysis of the likelihood of AC restoration vs time. However, it is clear that the most likely AC restoration times are before any point of no return. Thus, an upper bound on the improvement in the blackout melt sequence frequency attributable to feed and bleed is of the order of 10^{-6}/yr or less.

To summarize, the principal concerns regarding the CE designs with low HPI shutoff head and no PORV's appear to be:

1. Risk of core melt via loss of all feedwater may be unacceptably high.

2. The adequacy of the design for very small LOCA mitigation is questionable. This may be coupled with operator behavior issues.

3. The reliability of the high pressure injection system may be unacceptably low, but the mere fact of an AFW requirement to mitigate very small LOCA's - given design adequacy - does not significantly degrade the reliability with which very small LOCA's may be mitigated.
4. It is important that either diesel generator be capable of energizing a motor driven AFW train given loss of offsite power.

Two questions remain to be answered: (1) what is it worth to equip these plants with feed and bleed capability? and (2) what are the attendant risks of the optional fixes?

As assessment of the value of the fix follows. Those core melt accident sequences for which a feed and bleed capability could save the core are likely to be well-contained; they do not entail common mode failure mechanisms which would defeat containment isolation, sprays, or fan coolers. Thus the utility's economic risk dominates.

Let us take the cost of such a core melt event to be around $10 billion (low: $2 billion for TMI's; high: $100 billion for extensive shutdown orders). The value in $ is essentially:

$$V(\$) = \Delta\lambda \text{ (events per year)} \times C(\$ \text{ per event}) \times T(\text{exposure time in years})$$

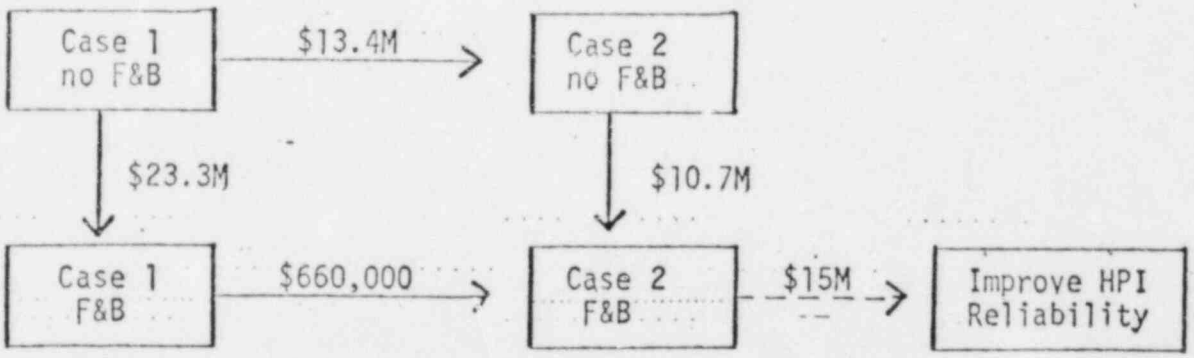
We can calculate a variety of $\Delta\lambda_{cm}$ differences from the following table:

λ_{cm}	Without Feed and Bleed	With Feed and Bleed
TML (first core)	9×10^{-4}	9×10^{-6}
TML (mature)	1×10^{-5}	1×10^{-7}
LOSP Case 1*	1.4×10^{-4}	1.8×10^{-5}
LOSP Case 2*	1.8×10^{-5}	1.2×10^{-5}
S_2D	1.509×10^{-4}	1.5×10^{-4}

*Case 1 - one of the diesel generators cannot energize a motor driven AFW train

Case 2 - both diesel generators can energize a motor driven AFW train

The economic incentives can be calculated by taking the exposure time for the first core as one year and for mature operation as ten years. The economic incentive is essentially the reduction in the present worth (at startup) of projected monitary losses due to accidents. They are shown on the following diagram:



This diagram can be understood as follows. Start with a CE plant that has no feed and bleed capability and only one diesel generator that can support a motor-driven auxiliary feedwater pump. It would be worth up to $13.4M to enable the second diesel generator to power what is now the non-safety grade AFW pump. It would be worth up to $22.3M to add feed and bleed capability, and so forth. The final "fix" has yet to be discussed. The value was arrived at by postulating design or operational changes such that the likelihood of an S_2D core melt is reduced from 1.5×10^{-4}/yr to 1.0×10^{-5}/yr. This might be achieved by either improving the reliability of HPI substantially, reducing the frequency of very small LOCA substantially, or some of each.

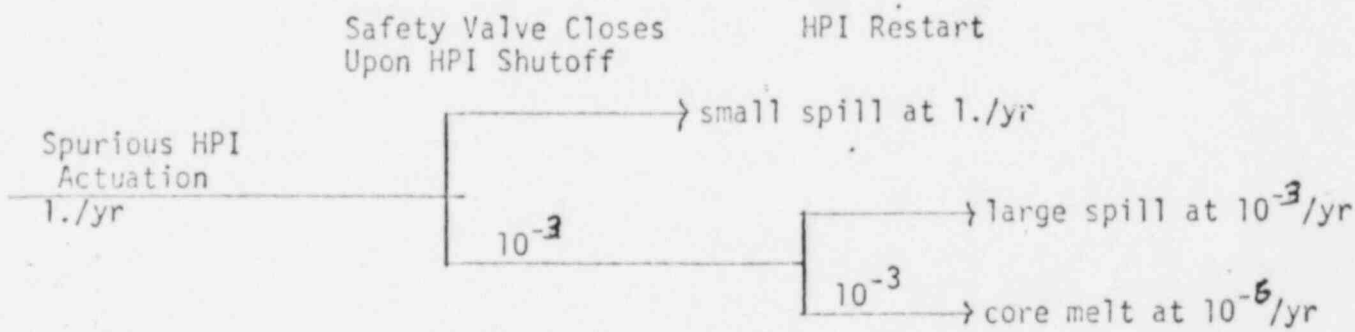
Now a feed and bleed capability could be achieved by installing suitably sized PORV's or by installing HPI pumps of very high head (over the pressurizer safety valve setpoint) or some of each. We have already examined the attendant risks of PORV addition. Care must be taken to design the control logic so that spurious "open" commands are rare, but it is safe to expect that this will be done well enough that the frequency of S_2 LOCA is not significantly increased. The effect on transient-induced LOCA is not important (this frequency is negligble with or without a PORV) and is compensated by the possibility of isolating PORV-LOCA's with the block valve.

If the HPI can force open a pressure relief valve (code safety or PORV in the pressurizer), then a spurious HPI actuation can cause a temporary, recoverable LOCA. Should the valve stick, we may have (without a block valve) a sustained LOCA. I assume that the operators will shut off HPI though not before a

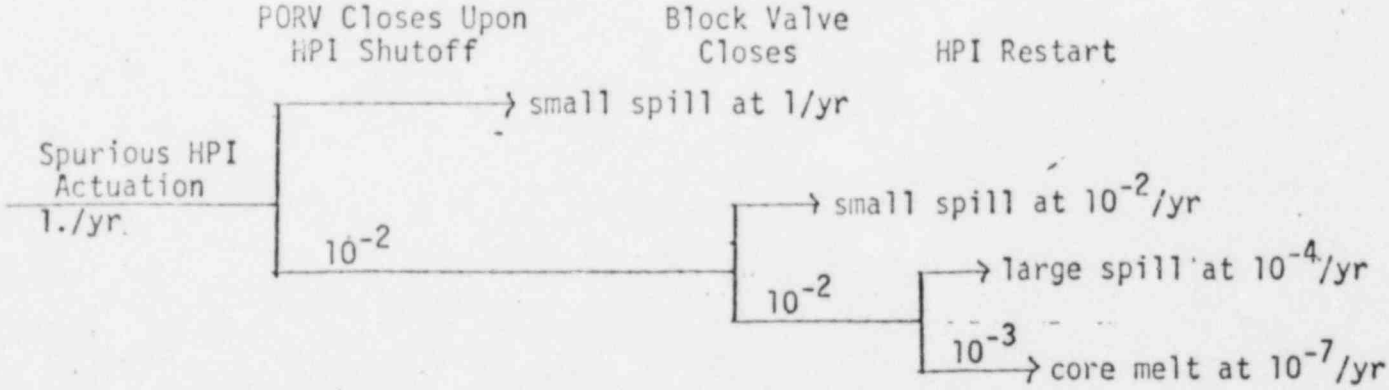
pressurizer valve opens, the pressurizer quench tank rupture disk blows, and a small spill occurs. If the valve sticks open (and cannot be isolated), the operators must restart HPI. Spurious HPI actuations are quite common. We assume here that the frequency of spurious HPI actuations which remain on long enough to challenge a pressurizer valve is one per year.

Borrowing from the prior analyses we can draw the following event trees for the high head HPI design:

Without PORV (or PORV left blocked)



With PORV installed and unblocked



Note that if a PWR has a PORV and high head HPI, it is better to run with the block valve open, so the isolatable PORV can take the brunt of spurious HPI actuations as well as feedwater transient-induced LOCA's. Note also that the core melt sequences caused by spurious HPI actuation in plants with high head HPI is acceptably small and can be made smaller still if the PORV only lifts (block valve left open). It is roughly balanced by comparable risk reductions in that for these designs, the PORV need not open to accommodate feed and bleed.

However, we should note that there is a real economic incentive to avoid the blown pressurizer quench tank rupture disk and the attendant small spills. If we assume a five day outage at one million dollars a day for small spills and a 100 day outage for a large spill, then the present worth of expected losses due to spurious HPI actuation in these designs is:

1 event/yr x 5×10^6 \$/event x 10 year exposure = \$50 million from the small, frequent spills with either design variant. For the large spills (unisolated LOCA) we have:

$$\left.\begin{array}{l}\text{Without PORV: } 10^{-3}/\text{yr} \\ \text{With PORV: } 10^{-4}/\text{yr}\end{array}\right\} \times 10^8 \text{ \$/event x 10 yr} = \left\{\begin{array}{l}\$10^6 \\ \$10^5\end{array}\right.$$

Thus utilities are subject to a significant incentive (present worth of projected losses of \$50 million) either to employ HPI pumps that cannot lift a pressurizer relief valve or to go after improved prevention of spurious HPI actuations or both.

There appears to be no economic penalty (other than first cost) in providing HPI pumps whose shutoff head is at normal RCS pressure, i.e., around 2250 psi.

In summary, then, this limited risk analysis cannot distinguish a difference in safety among the several ways to achieve feed and bleed capability: install one or more large PORV's, raise the HPI head above the pressurizer safety valve setpoint, or install a smaller PORV and raise the HPI head to near normal operating pressures. These choices must be made on the basis of design adequacy or thermal hydraulic considerations, preferably considering ATWS as well as the design to assure that very small LOCA's can be mitigated even though HPI or AFW may be late in starting or might be throttled temporarily by the operators. We have, however, found a plant availability incentive to avoid an HPI head so high that it can lift a pressurizer relief valve. No such penalty accrues to HPI designs with a shutoff head at the normal RCS pressure.