CT-1303
G-Q

ELBERT P. EPLER
NUCLEAR SYSTEMS CONSULTANT
712 FLORIDA AVENUE
OAK RIDGE, TENNESSEE 37830
483-0994

Dec 30 1980

J. Ray, Chairman
AC/DC Power Systems Reliability Subcommittee

In accordance with our recent conversation, I have reviewed NUREG 0666 "A Probabilistic Safety Analysis of DC Power Supply Requirements of Nuclear Power Plants". The study confirms that d.c. failure constitutes ½ of the probability of failure to remove residual heat and is therefore a significant contributor in need of correction.

The study however has examined a minimal d.c. system and, inasmuch as all plants employ more than the minimum, the finding must be regarded as being somewhat pessimistic. Therefore the proposed program for correction would, if successful, reduce core melt probability by less than a factor of two, and would seem not to justify a large expenditure of effort. By contrast the ATWS mitigation programs propose to reduce the probability of that mechanism by orders of magnitude.

Having corrected less than half of core melt probability by means of improvements to the d.c. system, other means must be sought to apply to the remaining larger fraction. It would be worthwhile to consider a single program that would reduce by significantly more than a factor of two, the probability of failure to remove residual heat.

In considering the contribution of heat removal to core melt probability, it is important to recognize the existence of a more urgent need. The Reactor Safety Study has pointed out that one core melt event is to be expected in 20,000 LWR years of operation but with evacuation procedures, prompt fatalaties would be expected in only one event in fifty. Now, after experiencing the Browns Ferry and TMI events, it becomes clear that the more urgent problem is the spectacle of the operator's struggles to remove residual heat by use of general purpose systems which have become damaged or unavailable, thus contributing greatly to the public's perception of nuclear risk.

The Browns Ferry and TMI events occurred at about the rate of one per 200 LWR years, a rate

100 times greater than the 20,000 LWR year rate for core melt. As a result, evacuation of the population is now being taken seriously, and if the 200 year rate were to persist, we might expect to see, with 200 LWRs in service, such events once per year, wherein the population within a ten mile radius of the plant would be evacuated. This would be entirely unacceptable. It is therefore urgently required that measures be adopted enabling residual heat removal without requiring the operator to struggle in the public view with systems that have become inoperable.

This subject is discussed in greater detail in ORAU/IEA 80-7(M) Research Memorandum "Common Mode Failure of LWR Systems: What Has Been Learned" Oak Ridge Associated Universities/Institute for Energy Analysis. Some of the more significant points are as follows.

During the reactor development period, over two dozen events occurred wherein a critical assembly became uncontrollable requiring that the excursion be terminated by violent dissassembly of the configuration. This led to an extensive program of

development of techniques for ensuring the reliability of the Reactor Shutdown System. These early reactors were small and the residual heat removal problem correspondingly small, so that off-the-shelf techniques for heat removal were deemed to be adequate. Over the years the reactivity excursion has been tamed by the dedicated Reactor Shutdown System, plus the doppler fuel temperature coefficient and the application of Zircalloy cladding capable of withstanding higher temperatures. Thus the reactivity excursion has become a minor problem while the removal of residual heat from the much larger LWRs has become the dominant problem. Off-the-shelf techniques may indeed have been adequate for the small early reactors, but we can no longer afford to ignore the techniques employed in controling the fission process wherein a dedicated, self contained system, which is used for no other purpose, performs without the need for operator intervention.

An important technique employed to obtain reliability is the application of two or more independent redundant trains. Existing systems for heat removal are required to meed the

single failure criterion, which does no more than to assure the application of redundancy. Much more than this however, is required to assure reliability. NUREG 0666 recognizes this and has pointed out that the existence of the bus tie breaker destroys the independence of the redundant d.c. trains, and recommends that its use be prohibited. There are, however, other more serious violations of good practice.

The vital d.c. services, which are essential for the operation of circuit breakers, valves and instruments, are also used to supply general purpose plant loads. As an example the large oil pumps, such as the turbine emergency lubricating system, have repeatedly overloaded and discharged the batteries. A dedicated heat removal system would prohibit the use of this vital service for any purpose other than for heat removal.

The failure of a protection system can be tolerated if the unavailability occurs at a time other than when protection is needed. For this

reason it has been recognized as important that the systems for control and protection be carefully separated so as to minimize the possibility of their concurrent failure. This separation has been referred to as "church and state". No such separation is employed in systems for residual heat removal. in fact, no separate system exists. As a result we have repeatedly seen the failure of a vital service, such as d.c., which has caused plant shutdown and in turn, the need for that service to operate breakers and valves for residual heat removal. True, only one of two trains would ordinarily become unavailable, but it is important that the plant, when forced into the residual heat removal mode of operation, from which there is no escape, have available two operable trains. (The utility would be cited for violation of tech. specs - if the reactor were to be started up with one train unavailable, and by shutting down, escape would in that case be possible) A separate dedicated system for residual heat removal would be incapable of causing plant shutdown.

In order for redundancy to be effective, it is necessary that component failures be detected

by periodic testing. It is required that such tests be performed without impairment of the ability to protect during or following the test. At TMI no such provision was incorporated in the design of the Aux Feedwater system. In fact it is alleged that the alignment of valves for testing was so unhandy that they were allowed to remain in the test position until the next test period. As a result the two electric trains and the turbine driven train were all valved out and unavailable when needed. It is to be noted that this would not be remedied by the proposal to improve the d.c. system. It is also noteworthy that testing if left entirely to the operators devices, can be downright dangerous. The Browns Ferry fire was caused by testing — with a candle.

These systems meet the single failure requirement but the designers have not adopted the principles employed in the design of a dedicated protection system, such as independence of redundant trains, use of protection features for no other purpose, separation of protection and control and provision for periodic testing without impairment of the ability to protect. Instead, heavy reliance has been

rested on the operator, given sufficient time, to maintain cooling using available alternatives which exist in considerable depth. Earlier studies such as NUREG 0305, emphasize that the second d.c. supply must fail within 30 seconds following the loss of offsite power, and this probability is less than 10^{-3}. The current study also emphasizes repeatedly that one hour is available to the operator for restoration of systems to normal operation, and thereby prevent core damage. These observations tend to encourage the belief that that the operator would succeed in spite of system failures. Operating experience, however, shows this to be highly optimistic as illustrated by the following examples.

At H. B. Robinson the parasitic turbine emergency lube oil pump remained on test beyond the allowable two hours and caused depletion of the battery charge. In spite of multiple warnings such as dim pilot lights and failure of the plant computer, the overload was allowed to persist until scram occurred, and as a result the turbine bearings were wiped out. Had the bus tie breaker been in the closed position

during this period, both batteries could have been discharged. In that case, offsite power would have been unavailable and both batteries would have failed before the 30 sec. allowable period. Further, in consideration of the inability of the operating staff to recognize the failing condition of the d.c. supply, had both buses failed and with a.c. power unavailable, it is unlikely that conditions would invariably be restored to normal within one hour. In the H.B. Robinson event the turbine bearings could have been saved had the operating staff, during the two hour period available, been able to recognize the problem and manually close circuit breakers to restore either the a.c or d.c. supply to the oil system.

At Quad Cities, again large parasitic loads caused the battery charger breaker to trip on overload, and at the same time the transient caused the reactor to scram. The tripped breaker was annunciated, but the operating staff believed the annuncintion to be spurious. The reactor was restarted with the battery charge depleted, and continued in operation for 21 hours. During this time with the charger unavailable,

the battery continued to be discharged by the parasitic loads. Finally, as a result of pipe vibration, an independent event, other failures occurred. As a result the plant became inoperable and was again forced to shut down as the reactor scrammed. Had the independent event, instead of pipe vibration and subsequent failures, been the failure of the second d.c. supply, again the plant would have been forced to shut down but with <u>both</u> d.c. supplies unavailable.

These examples do little to encourage the belief that the operator would invariably succeed or that one hour, or even 30 seconds, would always be available.

Like the Browns Ferry fire, there are many ways in which the general purpose plant systems might be damaged so as to make them incapable of removing residual heat, and at the same time, by causing plant shutdown, make residual heat removal necessary. Such occurrences would include large fires (including battery fires) explosions, hurricanes, and sabotage. These would not only damage the plant but might also drive the operator from the building. Thus a protected

self contained system for heat removal which would be unaffected by these conditions, and which would operate with the minimum of human intervention, would serve both to reduce the probability of core melt and, of more immediate benefit, minimize the need for precautionary evacuation of the population. There is, however, yet another important benefit to be derived by means of a dedicated and protected heat removal system.

The AEC had maintained the position that siting and safety were unrelated by reason that a serious accident to the plant could be ruled out as highly improbable. As a result of TMI, however, this position has been abandoned and NUREG 0625 outlines a new siting policy taking into account population density. Over half of plants now in operation or under construction, would not meet the proposed requirements. Some of these plants might be forced to shut down, others might continue operation with added safety features and all, or most, might be unsuitable for expansion. (This latter could be unfortunate as additional units are apt to be safer as a result of learning). It would

seem, therefore, that the addition of a dedicated system for residual heat removal that would minimize the need for evacuation, might be considered to be a reasonable price to pay to keep these plants in operation, and in some instances even allow the installation of additional units.

With these factors in mind it clearly would be desirable to initiate a study leading to the development of criteria for the addition of a dedicated and protected system to existing plants. The team conducting the study should include individuals thoroughly acquainted with the principles applied to the design of the Reactor Shutdown System, as well as an equally thorough understanding of heat removal hardware.

Some notion of the effectiveness of such a system might be obtained by a comparison with the Reactor Shutdown System, which like a heat removal system would be called upon to operate six or more times per year, although in many instances the main condenser would remain available for heat removal.

The Shutdown System, however, needs to respond only momentarily whereas a heat removal system must operate continuously over a long term, while depending on sources of electrical power and coolant. Residual heat removal is clearly the more difficult problem yet the Reactor Shutdown System has, in the ATWS matter, been held to be inadequate. On this basis the failure to remove residual heat might remain a major contributor to core melt, however the system should be eminently successful in minimizing the spectacle of the operator's struggles to remove residual heat by the use of general purpose plant systems which have become inoperable, and which not only becomes a media event, but in many instances would cause an unneeded evacuation of the population.

Finally, having recognized the need for a more conservative siting policy and a corresponding improvement in evacuation procedures, it would seem that no obstacle should remain to prevent the acknowledgement of the need for a dedicated and protected system for residual heat removal.