BNL-NUREG-63222
CONF-960912--32

TECHNICAL SPECIFICATION ACTION REQUIREMENTS FOR AFW SYSTEM FAILURES: METHOD DEVELOPMENT AND APPLICATION TO FOUR PWR PLANTS[a]

Tuomas Mankamo
Avaplan Oy
Itainen Rantatie 17
FIN-02230 Espoo
FINLAND

Inn S. Kim,[b] Ji Wu Yang, and Pranab K. Samanta
Brookhaven National Laboratory
Building 130
P.O. Box 5000
Upton, New York 11973-5000

ABSTRACT

Failures in the auxiliary feedwater (AFW) system of pressurized water reactors (PWRs) are considered to involve substantial risk whether a decision is made to either continue power operation while repair is being completed, or to shut down the plant to undertake repairs. Technical Specification (TS) action requirements for failures in the system, based on engineering judgements, usually require immediate plant shutdown in the case of multiple failures in the system (in some cases, immediate repair of one train is required when all AFW trains fail). In this paper, we present a probabilistic risk assessment (PRA)-based method to quantitatively evaluate and compare both the risks of continued power operation and of shutting the plant down, given known failures in the system. The method is applied to the AFW system for four different PWRs. The results show that the risk of continued power operation and plant shutdown both are substantial, but the latter is larger than the former over the usual repair time. This observation was substantiated for four plants with different designs: two operating Westinghouse plants, one operating Asea-Brown Boveri Combustion Engineering Plant, and one of evolutionary design. The method developed can be used to analyze individual plant design and to improve AFW action requirements using risk-informed evaluations.

1. INTRODUCTION

The auxiliary feedwater (AFW) system of a pressurized water reactor (PWR) has the important function of providing makeup to the steam generators for removing decay heat following a reactor trip or a loss of the main feedwater system. Also, during controlled shutdown, some PWRs are designed to use the AFW system in hot standby for removing residual heat. Technical Specifications (TS) usually require an immediate shutdown of the plant when there are multiple failures in the AFW trains, i.e., 2- or 3-train failures in the typically 3-train system (in some cases, immediate repair of one train is required after the failure of all AFW trains). With the availability of probabilistic risk assessment (PRA) models for nuclear power plants (NPPs), the risk associated with available alternatives can be quantitatively evaluated, and, as necessary, these requirements can be improved. Defining the action requirements for failures in the AFW system is helped by such an evaluation and comparison of the risks associated with the two main alternatives available: the risk of continued power operation while repairs are being completed, and the risk of shutting down the plant to perform repairs. We use core-damage frequency (CDF), and core-damage-probability (CDP) as the measure of risk in our evaluation.

Evaluating the risk of shutting down a plant involves considering the processes involved, the condition of the plant's decay heat, and the human actions associated with the transition from full power to shutdown. The PRA model developed for power operation cannot be directly used to quantify this risk. Shutdown PRAs[1-3] provide much useful information for evaluating this risk, but also may not have an adequate level of detail. Previously, detailed models were generated to quantify this risk.[4] The insights gained from them and their applications have allowed us to develop simplified models that are easier and less resource-consuming for plant-specific applications. The risk of continuing operation can be assessed relatively easily by the PRA model for full-power, after appropriately modifying the input data for inoperable equipment, and adjusting the model for conditional common-cause failure (CCF) events. In this paper, we describe the simplified method and its application to failures in the AFW system. Specifically, we present the following:

---

[a]Work performed under the auspices of the U.S. Nuclear Regulatory Commission. The views expressed are those of the authors and do not necessarily reflect any position or policy of the U.S. NRC.
[b]Currently with Korea Atomic Energy Research Institute, Taejon, Korea.

1) the methodology for evaluating the risk impact of the TS action requirements for both alternatives, i.e., continued power operation and plant shutdown,

2) the application of the method to analyze the risks of these operational alternatives in failures of the AFW system for four PWR plants: Surry 1, Sequoyah 1 (Westinghouse), San Onofre 3 (ABB-CE), and System 80+ (evolutionary).

Finally, we present our insights from these applications.

2. DESIGN OF THE AFW SYSTEMS AND PRESENT ACTION REQUIREMENTS

The AFW systems of three plants, Surry 1, San Onofre 3, and Sequoyah 1, have a similar configuration to most typical operating plants, consisting of two electric motor-driven pumps (MDPs) and one steam turbine-driven pump (TDP). The emergency feedwater (EFW) system of the System 80+ plant has two divisions, each of which consists of one MDP and one TDP. All four plants use the emergency condensate storage tank as the normal suction source, but all have alternate suction sources.

Of these four plants, Surry 1 is unique in that the main feedwater (MFW) system normally is used to remove core decay-heat from the primary system after a reactor trip or a controlled shutdown. Therefore, the AFW system normally is on standby until the reactor coolant system (RCS) cools down to about 345°F, at which point the residual heat removal (RHR) system can be used to further remove decay heat.

The action requirements of the TSs for the three operating plants are similar in that 1) 72 hours of allowed outage time (AOT) are provided for failure of one MDP or TDP, and 2) immediate plant shutdown is required for double failures. However, for triple failures, San Onofre 3 and Sequoyah TS require immediate action to restore them to operable status, while Surry 1 TS require immediate shutdown of the plant.

The action requirements for System 80+ differ from those for the other three plants because it has four EFW pumps. Hence, some AOT is provided for double failures at this plant. If both pumps (1 MDP and 1 TDP) are inoperable in the same division, then they both must be restored to operable status within 72 hours. If one EFW pump in each division is inoperable, then the operability of one of them must be restored within 72 hours. Where any three or all four EFW pumps are inoperable, then the TS for System 80+ require immediate shutdown of the plant, as in the case of double or triple failures at Surry 1.

3. METHODOLOGY

3.1 Concept of LCO Shutdown and Operating Risks

We consider two alternatives when an AFW system enters a limiting conditions for operation (LCO) because of the failure of one or more components in the system: a) continue power operation and repair the failed equipment within the defined AOT, or b) shut down the plant to complete the repairs in a shutdown state. We call these alternatives the basic operational alternatives, and call the risks associated with these alternatives the LCO risks. The risk associated with repairing the equipment while continuing power operation is called LCO operating risk; that associated with shutting the plant down is called LCO shutdown risk.

Figure 1 shows a conceptual plot of LCO operating and shutdown risks in terms of core-damage frequency for the failure of a system, like the AFW, which is needed to remove decay heat. At time A when the failure is detected, the two basic operational alternatives are applicable, i.e., continue power operation, and shut down the plant. The solid line represents the risk profile for continued operation, while the dotted line is the profile for shutdown.

Upon detecting the failure at time A, the LCO operating risk increases above the baseline due to the increased unavailability of the initially affected system (i.e., failed or degraded) during potential occurrences of accident scenarios requiring it to be operational to prevent core damage. The baseline represents the level of risk associated with power operation when no known failures exist.

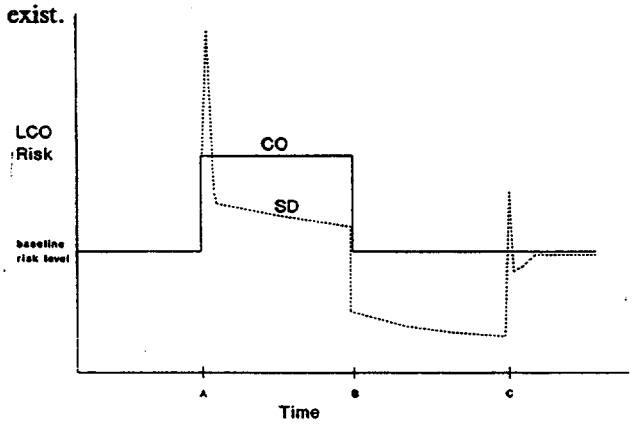

Figure 1 Comparison of LCO risks (core-damage frequency) for the basic operational alternatives of continued power operation and shutdown

DISCLAIMER

The initial increase in the LCO shutdown risk (Figure 1) results from the system's unavailability during potential occurrences of accident scenarios initiated by events occurring while the plant is being brought to shutdown. Specifically, the increase in risk in the initial stage of shutdown arises from 1) the unreliability of the systems which are needed during the change in plant's state, or which must be started up, and 2) the vulnerability of the plant to transients caused by the changes in the plant's state. After entering a stable shutdown state, the risk level usually decreases with time because of the diminishing decay heat, meaning that there are lower requirements for capacity on safety system, and a longer time available for recovery if a critical safety function is lost during a shutdown-cooling mission. The principal motivation of going to shutdown is to reach the lower level of risk in a stable shutdown mode, compared to the continued-operation alternative.

At time B, when the component is repaired and returned to service, both operating and shutdown risks decrease. The operating risk decreases to the baseline risk level, i.e., the level before the failure was detected, whereas the decrease in the shutdown risk depends on the baseline level corresponding to the shutdown state reached (e.g., hot shutdown) and may be lower or higher compared to the baseline in the power operation state. The CDF level depends on a number of competing factors: lower decay heat level, increased likelihood of some (loss of RHR and loss of offsite power) initiating event frequency, and disabled automatic actuation of some safety systems. Another small peak in the shutdown risk at time C arises from the unavailabilities of systems that are needed when the plant is restarted up, and the plant's vulnerability to transients that may be caused by the changes in the operational mode. In this period, the risk is also a function of the rate of heat production, as represented by a small dip in the dotted line which then slowly increases to the baseline risk level as the plant reaches full power operation.

The period that is directly relevant to evaluating action requirements or AOTs for failures in the safety systems is from time A to B, i.e., the predicted or actual repair time for the component. The risk over this period, i.e., core-damage probability, can be obtained by integrating the conditional CDF to compare the LCO operating and shutdown risks. If the former is smaller than the latter, then from a risk point of view, the alternative of continued operation is preferable to the shutdown alternative, and vice versa.

3.2 Method for Quantifying LCO Shutdown and Operating Risks

As discussed above, the LCO shutdown risk is incurred by initiators occurring while the plant is being brought to, or while in, shutdown. In the approach used to quantify LCO shutdown risks, the detailed time-dependence within each phase of the LCO shutdown is simplified by linearizing the shutdown phases piecewise. A previous study on the RHR and standby service water (SSW) systems of a boiling water reactor,[4] using a detailed model of the shutdown phases, provided insights on linearizing the shutdown phases such that the impact on the results is minimal; this is similar to the approach taken in low power and shutdown PRA studies,[2,3] but is more focussed on the transition phase from full power to shutdown, given failure in relevant systems. Low power and shutdown PRAs have usually placed less emphasis on this phase of operation, and accordingly, the models are not readily usable for TS applications. Nevertheless, quantification of LCO shutdown risk is greatly facilitated by the availability of such PRAs.

Two categories of initiating events may occur during an LCO shutdown:

a) Spontaneous time-correlated events which are quantitatively described by conditional frequency, and

b) Phase change-correlated events, which are quantitatively described by the likelihood of undesirable events occurring when entering or passing through a given phase, irrespective of the time spent in the phase.

The latter events may be caused by a latent defect which was not a problem in the preceding operation, but becomes critical when entering a specific shutdown stage. For example, a latent fault in the feedwater-regulating equipment may trip the feedwater pumps when flow is reduced. Events correlated with changes during shutdown include the loss of offsite power involving the loss of external grid due to an abrupt disconnection of the plant, triggered by a turbine trip. Human errors during shutdown operations also belong in this category.

There are four phases the plant will go through to complete the repair until it reaches the cold shutdown state: power state, power reduction, hot standby, and hot shutdown. The power state applies to the alternative of continued power operation. When the shutdown alternative is taken, then the plant will enter the phases of power reduction, hot standby, and hot shutdown. The power reduction phase starts from the time the plant initiates

action to go to shutdown until it reaches subcriticality. In this study, the hot shutdown is assumed to be the end state.

The classification also applies to the failure modes of safety systems. For example, failure to start a normal shutdown cooling system falls into phase change-correlated events, while the system's failure to continue operation falls into spontaneous time-correlated events.

We assessed the risk impact associated with a controlled shutdown with the equipment inoperable by considering the relevant initiating events for each defined phase of shutdown. The core-damage frequency for each phase of the LCO shutdown, which is incurred by spontaneous time-correlated events, can be represented as the following:

$$R(k) = \sum_i f(k)\, P_r(k)\, c_n(k)$$

where the summation is over all relevant initiating events with k denoting a phase of LCO shutdown, and

- $R(k)$ = the average core-damage frequency incurred while the plant is in phase k
- $f(k)$ = the frequency of spontaneous time-correlated events
- $P_r(k)$ = the plant's response
- $c_n(k)$ = the recovery credit factor

Correspondingly, the core-damage probability, which is incurred by phase-change-correlated events when changing phases, can be represented as:

$$r(k) = \sum_i p(k)\, P_r(k)\, c_n(k)$$

where the summation again is over all relevant initiating events with k denoting the phase of LCO shutdown the plant is entering, and

- $r(k)$ = the contribution to core-damage probability incurred when entering phase k
- $p(k)$ = the probability that phase change-correlated events will occur when entering phase k

In these expressions, f(k), p(k), $P_r(k)$, and $c_n(k)$ are all conditional on a given initiator. However, for simplicity, the initiator is not explicitly indicated in the expressions. References 5 and 6 have a detailed discussion of the evaluation of these variables.

The failures are assumed to be detected during normal power operation, with no other failure of safety systems known to be present. We assumed staggered testing and, hence, in an assumed failure combination of pump trains, the remaining trains are in standby and not tested following the detection of failure(s). This meant that the unavailability of the remaining part of the AFW system is given by a conditional probability, taking into account potential CCFs between the failed and remaining pump trains.

The risk impact of shutting down a plant with multiple failures in the AFW system can be represented as follows, based on the definition presented above, introducing a subscript representing a failure condition:

- $R_x(k)$: conditional core-damage frequency in phase k, given failure x, (x refers to different failure combinations, such as 1 MDP, 1 MDP and 1 TDP, 2 MDPs, etc.)
- $r_x(k)$ = conditional core-damage probability due to phase change-correlated sequences when entering or passing through phase k, given failure x,
- $P_{x,i}(k)$ = plant response: the conditional probability of core-damage, given failure x for initiating event i in phase k.
- $c_{x,i}(k)$ = recovery credit factor: the relative reduction in the conditional probability of core-damage sequences due to the increasing time window for recovery in phase k, given failure x for initiating event i,

then,

$$R_x(k) = \sum_i f_i(k)\, P_{x,i}(k)\, c_{x,i}(k),$$

$$r_x(k) = \sum_i p_i(k)\, P_{x,i}(k)\, c_{x,i}(k).$$

The core-damage probability for failure x in the AFW system for the shutdown alternative, assuming three phases for shutdown, can be expressed as:

$$r_{SD} = r_x(1) + R_x(1)\,\bar{t}_1 + r_x(2) + R_x(2)\,\bar{t}_2 + r_x(3) + R_x(3)\,\bar{t}_3$$

where $\bar{t}_k$ = the mean duration of phase k.

The risk of continued operation was assessed using the full power PRA by running the computerized PRA code after appropriately modifying the unavailability of the failed equipment and the common-cause model involving the component.

Let

r_{co} = the core-damage probability associated with continued power operation over the downtime of the equipment.

R_{co} = the increased core-damage frequency associated with continued power operation with the failed equipment.

$\bar{d}$ = the mean downtime

then,

$$r_{co} = R_{co}\ \bar{d}.$$

In the analysis, we assume that when the plant undertakes the LCO shutdown, it will be in the power reduction phase for 3 hours, and in the hot standby phase for the next 5 hours. The hot shutdown is assumed to start about 8 hours after initiating the LCO shutdown. The mission phase of hot shutdown is divided into 8-16 hours, and beyond 16 hours, to give adequate credit to the lower level of decay heat which means more recovery options and a smaller non-recovery factor. To compare the risk of continued operation with that of shutting down, the same duration is considered for both alternatives, i.e., if 24 hrs. of downtime is considered for power operation, then 24 hrs. is considered for shutdown which is divided into different phases, as discussed above.

4. APPLICATIONS

This section presents the results of evaluating the LCO operating (CO) and shutdown (SD) risks for failures in the AFW systems of San Onofre 3, Sequoyah 1, System 80+, and Surry 1, using the methodology discussed in Section 3.

As an example, Figure 2 shows the LCO operating and shutdown risks in terms of CDF and cumulative CDP for the failure of 2 motor-driven (MD) pumps at the Sequoyah plant. When the failure of the 2 MD pumps is detected at time zero, the two basic operational alternatives are applicable. The baseline represents the level of risk associated with power operation when no known failure exists. If the CO alternative is taken, the increase in CDF is shown by AB:CO line. However, if the SD alternative is taken, then the plant incurs a CDF higher by more than an order of magnitude than the corresponding CDF for the CO during the initial transition period of power reduction and state change. The plant will become vulnerable again to transients that may occur while entering the power reduction and hot shutdown states (the two SD risk peaks). After this initial increase, the CDF for the SD operation declines slowly because of the slow decrease of decay power during hot shutdown.

The cumulative risks of CDP are included in Figure 2, which shows that the SD risk remains larger than the risk of CO for an extended period. Comparisons of risks for the failure of other pump-train systems at the other three plants are similar to the risk profiles illustrated in Figure 2 for the failure of 2 MD pumps.

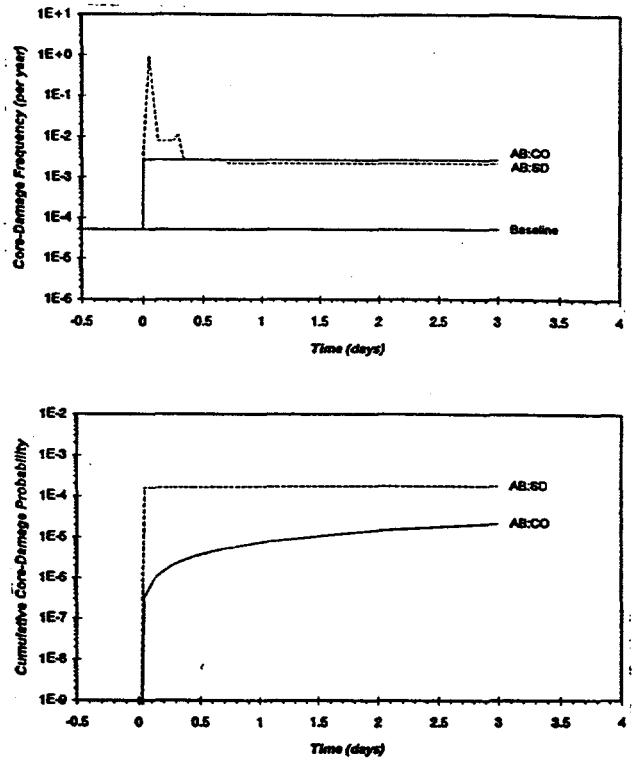

Figure 2 Comparison of CDF and CDP for the continued power operation (CO) and plant shutdown (SD) alternatives in failure of 2 motor-driven AFW trains at the Sequoyah plant

Based on such evaluation of each for the four plants, we obtain the following for each of them:

a) the core-damage frequency (CDF) in the power operation state,
b) the increase in CDF for failure in the AFW system in power operation state, and the ratio of increased CDF to the base case CDF (obtained in Step a), called the risk increase factor,
c) the CDF levels as the plant is shut down, given failure in the AFW system,

d) the integrated core-damage probability (CDP) over a repair time for continued operation and plant shutdown (r_{SD} and r_{CO}, as discussed above), and
e) the ratio of r_{SD} and r_{CO} over the same duration.

The risk increase factor represents the factor increase in CDF at power operation because of failures in the system; the ratio of risk for shutting down to continued operation (r_{SD}/r_{CO}) gives a perspective on the relative values of these parameters for different failure combinations in the AFW system. The ratios were obtained using a repair time of 24 hrs. for all train combinations. Table 1 summarizes the risk increase factors for power operation, and the ratio of r_{SD} and r_{CO} for the four plants. These risk measures are presented for single, double, and triple failures of the AFW systems for the four plants; for system 80+, quadruple failures also are considered because this plant has four EFW pumps.

The following summarizes the results of the risk evaluations given in Table 1:

1) Failure of a single AFW pump-train during power operation causes a relatively small increase in core-damage frequency over the baseline. An exception is one MDP failure in San Onofre 3 which causes more than an order of magnitude increase.

2) Multiple (i.e., double or triple) failures of the AFW trains at San Onofre 3, Sequoyah 1, and Surry 1 incur a large risk for both SD and CO alternatives, with triple failures causing much higher risk than double failures.

3) The r_{SD}/r_{CO} ratios range from 4 to 300. Therefore, shutting down the plant, given AFW failures, results in a larger contribution to core-damage probability than continued power operation with a degraded AFW system.

Based on these results, priority may be given to restoring the status of an inoperable train in the AFW system during power operation to minimize the risk impact of failures in the system. For this, a reasonable AOT may be provided especially for multiple AFW failures, as opposed to the present TS requiring immediate plant shutdown, at the same time, measures may be taken to detect multiple failures early, and to shut down the plant if at least one of the trains cannot feasibly be repaired within a short time.

Table 1 Summary of Risk Evaluation for AFW Pump Train Failure Situations for 4 PWR Plants

LCO State	Surry 1		San Onofre 3		Sequoyah 1		CE System 80+	
	Risk Increase Factor (Power Operation)	Risk Ratio r_{SD}/r_{CO}	Risk Increase Factor (Power Operation)	Risk Ratio r_{SD}/r_{CO}	Risk Increase Factor (Power Operation)	Risk Ratio r_{SD}/r_{CO}	Risk Increase Factor (Power Operation)	Risk Ratio r_{SD}/r_{CO}
1 MDP	2.6	7.8	10.3	17	5.4	19	1.7	296
2 MDP	19	5.6	120	18	52	23	4.5	147
1 TDP	2.8	5.7	2.7	13	2.2	14	1.6	311
1 TDP & 1 MDP	19	4.3	75	17	58	17	12	84
1 TDP & 2 MDP	230	4.2	880	18	680	23	172	49
2 TDP	-	-	-	-	-	-	10.4	67
2 TDP & 1 MDP	-	-	-	-	-	-	126	53
2 TDP & 2 MDP	-	-	-	-	-	-	1800	45

*MDP = motor-driven pump, TDP = turbine-driven pump, CO=continued power operation, SD=shutdown

5. SUMMARY

The insights from risk analysis of the AFW failures in the four plants can be summarized as follows:

1) The LCO operating and shutdown risks associated with failures in the AFW systems are both substantial, but the risk of shutting down the plant is larger than continuing power operation over a usual repair time. This observation was substantiated for all four plants with different designs: two operating Westinghouse plants, one operating ABB-CE plant, and an evolutionary reactor design. In most cases, the difference between the two risks is greater than the typical uncertainty ranges associated with such evaluations. Hence, we may reasonably assume that this conclusion is generally applicable to the operating PWR nuclear power plants.

2) These observations lead us to consider modifying the action requirements for the AFW systems to allow short repairs to avoid plant shutdown, and to incorporate testing requirements to detect multiple failures. The modifications should be directed at reducing the total risk impact associated with such failures.

In summary, we have presented a method for risk-based evaluation of the action requirements for failures in the AFW systems of a PWR, quantitatively considering both the risk of continuing operation and that of shutting down the plant. The results show that the risk associated with both the options are substantial, especially for multiple failures, where the risk of shutting down is larger than continuing operation for some duration, depending on plant-specific designs. Using such evaluations, TS action requirements can be evaluated and improved to be more risk-effective. The risk-effective action may include additional testing to detect multiple failures when single failures are detected, allowed outage times to complete the repair of one of the trains when such repair can be completed within a short time, e.g., 24 hrs., and early controlled shutdown when repair is expected to take a long time.

6. REFERENCES

1. D.C. Bley, J.W. Stetkar, L.A. Bowen, et al., "Zion Nuclear Plant Residual Heat Removal PRA," Nuclear Safety Analysis Center, NSAC-84, July 1985.

2. T.L. Chu, Z. Musicki, P. Kohut, et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit 1: Analysis of Core Damage Frequency from Internal Events During Mid-Loop Operations," NUREG/CR-6144, BNL-NUREG-52399, June 1994.

3. D.W. Whitehead, J. Darby, B. Staple, et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1," NUREG/CR-6143, Sandia National Laboratories, June 1994.

4. T. Mankamo, I.S. Kim, and P.K. Samanta, "Technical Specification Action Statements Requiring Shutdown: A Risk Perspective with Application to the RHR/SSW Systems of a BWR," NUREG/CR-5995, BNL-NUREG-52364, November 1993.

5. P.K. Samanta, I.S. Kim, T. Mankamo, et al., "Handbook of Methods for Risk-Based Analyses of Technical Specifications," NUREG/CR-6141, BNL-NUREG-52398, December 1994.

6. I. Kim, T. Mankamo, J. Yang, S. Gibelli, and W. He, "Action Requirements for AFW System Failures: An Analysis for Four Nuclear Power Plants," Draft Report, Brookhaven National Laboratory, June 1995,