NOTICE
PORTIONS OF THIS REPORT ARE ILLEGIBLE.
It has been reproduced from the best available copy to permit the broadest possible availability.

BNL-NUREG--35760

TI85 007620

A COMPARATIVE ASSESSMENT OF SELECTED PWR AUXILIARY FEEDWATER SYSTEM RELIABILITY ANALYSES*

R. Youngblood, A. Fresco, I. A. Papazoglou
Department of Nuclear Energy
Brookhaven National Laboratory
Upton, New York 11973

J. Tsao
U. S. Nuclear Regulatory Commission
Washington, DC 20555

MASTER

This paper presents a sample of results obtained in reviewing utility submittals of Auxiliary Feedwater System reliability studies. These results are then used to illustrate a few general points regarding such studies. The submittals and reviews for operating license applications are quite significant in that they represent an application of probabilistic risk assessment techniques in the licensing process.

After the accident at Three Mile Island, studies were performed of the Auxiliary Feedwater Systems (AFWS) of all then-operating PWR plants. Results for Westinghouse plants were presented in NUREG-0611 (1), and results for C-E plants were presented in NUREG-0635 (2). Generic failure data and maintenance data were applied, and a restricted set of failure modes was considered. The probability that the AFWS would fail to perform its mission (hereafter "AFWS unavailability") was estimated for three cases:

1. loss of main feedwater (LMFW);
2. loss of offsite power (LOOP); and
3. loss of offsite and onsite AC (LOAC).

*This work was performed under the auspices of the U.S. Nuclear Regulatory Commission.
Views expressed in this paper do not necessarily represent official NRC policy.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Since then, each applicant for an operating license has been required (3) to submit a reliability analysis of the plant's AFWS, carried out in a manner similar to that employed in the NUREG-0611 and NUREG-0635 studies. A quantitative criterion for AFWS reliability has been defined by the NRC in the current Standard Review Plan (SRP) for Auxiliary Feedwater Systems (4):

> "...An acceptable AFWS should have an unreliability in the range of 10^{-4} to 10^{-5} per demand based on an analysis using methods and data presented in NUREG-0611 and NUREG-0635. Compensating factors such as other methods of accomplishing the safety functions of the AFWS or other reliable methods for cooling the reactor core during abnormal conditions may be considered to justify a larger unavailability of the AFWS."

Some of the submittals have been sent to BNL for review. The BNL reviews (5-13) attempt, within a limited scope, to judge the completeness of the analyses and the quantification of the system unavailability with respect to the standard set in NUREG-0611. Results are modified as necessary by BNL to bring them into line with NUREG-0611.

Although stylized and limited in scope, these reviews have provided a useful framework for regulatory discussion of the various AFWS designs. In the remainder of this paper, some general points are made which should be useful in forming perspective on the results, in considering how to improve the process, and in preparing the submittals within the current framework.

APPLICATION OF THE SRP CRITERION

The SRP refers to an unavailability of 10^{-4} "per demand" as representing the upper end of the contemplated range of unavailabilities. The type of demand contemplated is not spelled out. There are arguments in favor of preferring a figure of merit based on loss of offsite power; LOOP scenarios have emerged from a number of PRAs as being significant contributors both to core damage and to risk.

It is certainly clear that the 10^{-4} per demand criterion cannot be construed to apply to the third case considered in NUREG-0611 and NUREG-0635, i.e., total loss of all A.C. power (LOAC). In nearly all plants either operating or under construction, the LOAC power situation is dealt with by a single steam turbine-driven or, in some cases, a diesel-driven pump train. Using the data and methodology of the subject NUREGs, any single pump train will be assigned a demand unavailability of at least 1E-2.

In these reviews, attention has been focused more on the LOOP case. This should be borne in mind as the following points are considered.

ACCOUNTING FOR ALLOWED MAINTENANCE

There are several points to be made here about the contribution of maintenance outage to system unavailability. It will be useful to discuss the following oversimplified case. Consider a system consisting of three trains A, B, C, any one train of which can fulfill the system's requirement.

Let q_i = unavailability of train i,

q_i^H = unavailability of train i, due to hardware failure,

q_i^M = unavailability of train i, due to maintenance outage.

Then, one can represent system unavailability by the following Boolean equation:

$$\overline{A} = q_A * q_B * q_C = (q_A^H + q_A^M) * (q_B^H + q_B^M) * (q_C^H + q_C^M)$$

$$= q_A^H * q_B^H * q_C^H + q_A^H * q_B^H * q_C^M + q_A^H * q_B^M * q_C^H + q_A^H * q_B^M * q_C^M + q_A^M * q_B^H * q_C^H + q_A^M * q_B^H * q_C^M$$

$$+ q_A^M * q_B^M * q_C^H + q_A^M * q_B^M * q_C^M \qquad (1)$$

Many of the terms in (1) correspond to multiple trains being out for maintenance. Consider first the contribution from terms having at most a single train out for maintenance. In this limited "proper" set of four terms, one term is pure hardware, and the other three are each partly maintenance. If large maintenance outages are assumed, maintenance terms will be a very significant contribution. NUREG-0611 mandates a non-negligible maintenance outage. Not all submittals have followed this (some assume much less maintenance), and one possible reason is evident from the above. Building in a standardized, sizable maintenance contribution for all plants has a noticeable effect on the results.

Half of the terms in (1) correspond to maintenance acts which are presumably improper, in that they cause multiple trains to be unavailable. If the numerical value of maintenance unavailability is on a par with hardware failure, blindly applying (1) can easily overstate unavailability by a factor of two or so.

One way of handling this is to incorporate NOT logic into the fault trees. This can be extremely clumsy. Another way is manually editing computer results to get rid of the undesired contribution. The easiest way is simply to neglect the "conservatism"; some submittals have been performed this way. One problem with the latter course of action is that it complicates the comparison between different AFWS designs. Another is that the results for the LOOP case can be especially distorted by this, sufficiently so to raise questions about why the unavailability is high. Here, we point out that straightforward application of one of the many useful features of SETS (14) can save the analyst a good deal of time.

First, form a new Boolean top event which describes maintenance on multiple trains. In the present example,

$$\text{MULTI-MAINT} = q_A^M * q_B^M + q_A^M * q_C^M + q_B^M * q_C^M \qquad (2)$$

Event MULTI-MAINT occurs if two or more trains are out for maintenance. Having formed MULTI-MAINT we now wish to eliminate from (1) any term which contains any of the terms of MULTI-MAINT. SETS contains a command (DLTRM) which does precisely this.

Thus, one's fault tree model is constructed without the annoyance of NOT logic. The computer spends a little extra time generating a number of illegal terms, and a little more time eliminating them with DLTRM, but the saving in human labor is worthwhile. This has enabled BNL to re-estimate and, in some cases (7), reduce the unavailabilities quoted by utilities which tended to penalize their designs.

If testing can also contribute to train unavailability, a trivial extension of the above procedure can easily handle multiple test acts or combinations of test and maintenance.

For purposes of standardization, NUREG-0611 mandates maintenance unavailabilities for certain classes of components. However, in certain configurations, these components cannot realistically be expected to require the indicated amount of maintenance. As indicated above, maintenance unavailability can be a substantial contributor to the calculated system unavailability, and blind application of (for example) the indicated maintenance unavailability of 2×10^{-3} for all valves, as seen in some submittals can severely distort the conclusions. As illustrations, consider the following two cases.

In the AFWS shown in Figure 1, maintenance on the single, locked-open, manually-operated valve near the Condensate Storage Tank (CST), 3CE-V27SAB-1, would require

isolation of all three pumps from the CST by closure of the manual valves on the individual suction lines as well as drainage of the CST itself, if it is assumed that maintenance requires physical removal of the valve from the line for repair or replacement. This would then force reliance on the non-condensate grade Emergency Water System as a source of auxiliary feedwater. Besides this, there would be a significant effect on the calculated unavailability because of the reduction in the redundancy of suction sources.

An even more vivid example of the effects of maintenance can be seen by again referring to Figure 1. Assuming that maintenance requires physical removal of any one of the motor-operated valves closest to the steam generators, downstream isolation would depend on the single check valve adjacent to the steam generator. It is presumably inappropriate to assume that this type of operation would be performed at the indicated frequency.

The previous two examples illustrate the necessity of defining a realistic maintenance policy for incorporation into the reliability analysis. The two major elements of such a policy are what types of valves or other components will typically undergo maintenance during plant operation and at what frequency and duration. The NUREG data are taken from WASH-1400 (15) and make no distinction between types of valves nor between pumps utilized in systems that are normally operating as opposed to being on a standby status. It would seem that pumps on standby status will require significantly less maintenance than pumps that are normally operating. Of course, the idle condition can also cause unique maintenance problems, but there is no a priori reason to assume that the maintenance frequencies should be equal for the two conditions. Similarly, manually-operated valves that are in a static system at ambient pressure and temperature are not likely to require frequent maintenance as opposed to motor-operated valves in a flowing system at high pressures and temperatures which are frequently exercised during normal plant operation.

Finally, a distinction should be made between scheduled and unscheduled maintenance acts. In the case of AFWS, scheduled maintenance is likely to be necessary only at very long intervals because of the normally idle condition of the system, so that any such maintenance can be deferred until shutdown. Obviously, normally operating systems can frequently require scheduled maintenance during plant operation.

The BNL reviews have adopted a policy of applying NUREG-0611 maintenance unavailabilities except to components whose type and placement clearly reflect an expectation of infrequent maintenance, as in the examples discussed above.

HUMAN ACTS AND ERRORS

While there are many aspects of the NUREG data pertaining to human acts and errors which are worthy of discussion, only the case of locked-open manual valves will be mentioned here. Table III-2 of NUREG-0611 indicates that, for acts and errors of a pre-accident nature, the probability that an operator inadvertently leaves a correct valve in the wrong position is 5E-4/demand if there is control room position indication, 5E-3/demand if there are local walk-around and double check procedures, and 1E-2/demand if there is none of the preceding.

The Standard Technical Specifications state that at least once per 31 days the position of each non-automatic valve in the flow path that is not locked, sealed, or otherwise secured in position must be verified. This implies that locked-open manual valves should be treated in Table III-2 as having neither control room position indication nor local walk-around and double-check procedures. The result is a higher error probability than if the valves are not locked open.

The BNL approach has been to assume that the locked-open case is equivalent to the local walk-around and double check case, or an error probability of 5E-3/demand. This is then modified by a recovery factor of 0.25 if either the valve's position is inherently indicated by the testing of the pump train, as in the case of a valve on the pump suction side, or if the operator can reasonably diagnose and recover from an incorrect position within 30 minutes of automatic AFWS initiation.

NONSAFETY-GRADE THIRD TRAINS

Some analyses of two-train systems have tried to take credit for nonsafety startup pumps serving as third trains (8,9,10). This has generally been a stumbling block, because (a) the scope of operator action generally necessary to bring such a pump on line was not contemplated in NUREG-0611, (b) the power supply to such a pump is sometimes not diesel-backed, or is a discretionary load on the diesels, (c) some of the hardware in such a "train" may have contributed to the initiating event which the AFWS is being challenged to mitigate, e.g., LMFW occurring during startup caused by failure of the startup pump itself, (d) flow control through the MFW flow paths is often dependent on availability of instrument air, supplied by compressors which are also a discretionary load on the diesels, and (e) the startup pumps are not ordinarily subjected to technical specification outage limitations. Thus, failure of such a "train" must be properly conditioned on the character of the initiating event. These factors have led, in some cases, to substantial delay in the review process.

TWO-TRAIN B&W VS THREE-TRAIN WESTINGHOUSE

Table 1 includes a comparison between a two-train B&W AFWS and a three-train Westinghouse system. It must be noted that several B&W reports have argued against naive comparisons of this type, which are to be viewed with caution. The figures quoted on Table 1 reflect a top event definition which, in effect, assumes that the operators have insufficient time in the B&W plant to back up AFWS actuation or recover from other hardware failures before dryout occurs. In the Westinghouse case, on the other hand, substantial credit for operator action has been given, based on a longer time available before dryout. This has a very substantial effect on the results. The comparison would change considerably if a less stringent top event definition were considered, e.g., if dryout for a brief period were not considered "failure" in the B&W plants. Other features of the mission success definition also serve to complicate this comparison. The "dryout" criterion, however, is written into NUREG-0611.

SUMMARY

Generally, AFWS unavailability given LOOP is the figure of merit to which the most attention has been given. One sees that two-train plants have great difficulty meeting the SRP standard. Taking credit for a startup pump helps in some cases, but a number of technical questions arise which substantially complicate the review process.

A convenient way to eliminate double maintenance and/or test contributions has been mentioned; eliminating these is important because, especially for the LOOP case, failure to eliminate double maintenance places the design in an artificially unfavorable light. The need for more explicit guidance regarding maintenance policy has also been discussed.

One aspect of the assumptions for human acts and errors vis-a-vis locked-open manual valves has also been touched upon.

REFERENCES

1. USNRC, "Generic Evaluation of Feedwater Transients and Small Break *Loss-of-Coolant Accidents in Westinghouse Designed Operating Plants,*" NUREG-0611, January 1980.

2. USNRC, "*Generic Evaluation of Feedwater Transients and Small Break* Loss-of-Coolant Accidents in Combustion Engineering Designed Operating Plants," NUREG-0635, January 1980.

3. Letter from D. F. Ross, Jr., USNRC, to "All Pending Operating License Applicants of Nuclear Steam Supply Systems Designed by Westinghouse and Combustion Engineering," March 10, 1980.

4. USNRC, "Auxiliary Feedwater System (PWR)," Standard Review Plan 10.4.9, Rev. 2, NUREG-0800, July 1981.

5. R. Youngblood and I. A. Papazoglou. "Review of the Crystal River Nuclear Generating Station Unit No.3 Emergency Feedwater System Reliability Analysis." NUREG/CR-3081, BNL-NUREG-51626, Brookhaven National Laboratory, October 1983.

6. A. Fresco, R. Youngblood, and I. A. Papazoglou. "Review of the Vogtle Units 1 and 2 Auxiliary Feedwater System Reliability Analysis." Draft Report, Brookhaven National Laboratory.

7. A. Fresco, R. Youngblood, and I. A. Papazoglou. "Review of the Catawba Units 1 & 2 Auxiliary Feedwater System Reliability Analysis." NUREG/CR-3297, BNL-NUREG-51675, Brookhaven National Laboratory, October 1983.

8. A. Fresco, R. Youngblood, and I. A. Papazoglou. "Review of the Seabrook Units 1 & 2 Auxiliary Feedwater System Reliability Analysis." NUREG/CR-3531, BNL-NUREG-51723, Brookhaven National Laboratory, February 1984.

9. R. Youngblood and I. A. Papazoglou. "Review of the Byron/Braidwood Units 1 & 2 Auxiliary Feedwater System Reliability Analysis." NUREG/CR-3096, BNL-NUREG-51633, Brookhaven National Laboratory, November 1983.

10. R. Youngblood and I. A. Papazoglou. "Review of the Davis-Besse Unit No.1 Auxiliary Feedwater System Reliability Analysis." NUREG/CR-3530, BNL-NUREG-51722, Brookhaven National Laboratory, February 1984.

11. R. Youngblood and I. A. Papazoglou. "Review of the Arkansas Nuclear One Generating Station Unit No.1 Emergency Feedwater System Reliability Analysis." NUREG/CR-3529, BNL-NUREG-51721, Brookhaven National Laboratory, February 1984.

12. D. Ilberg, R. Youngblood, and I. A. Papazoglou. "Review of the Rancho Seco Nuclear Generating Station Unit No.1 Auxiliary Feedwater System Reliability Analysis." NUREG/CR-3013, BNL-NUREG-51620, Brookhaven National Laboratory, April 1983.

13. A. Fresco, R. Youngblood, and I. A. Papazoglou. "Review of the Shearon Harris Units 1 and 2 Auxiliary Feedwater System Reliability Analysis." Draft Report, Brookhaven National Laboratory, October 1983.

14. R. B. Worrell and D. W. Stack. "A SETS Users Manual for the Fault Tree Analyst." NUREG/CR-0465, Sandia National Laboratory, November 1978.

15. USNRC, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants--Appendices 3 & 4: Failure Data," WASH-1400 (NUREG 75/014), October 1975.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Table 1

COMPARISON OF DEMAND UNAVAILABILITIES FOR TYPICAL AFWS DESIGNS (5,6,8)

AFWS Design	Unavailability/Demand			
	Utility		BNL	
	Avoid Dryout	Supply AFW Within 20 Min.	Avoid Dryout	Supply AFW Within 20 Min.
1. 2-train plant with B&W NSSS				
a) LMFW	5.7×10^{-5}	7.4×10^{-6}	1.4×10^{-3}	5.4×10^{-4}
b) LOOP	3.3×10^{-4}	1.5×10^{-4}	2.8×10^{-3}	1.3×10^{-3}
c) LOAC	1.4×10^{-2}	7.6×10^{-3}	3.9×10^{-2}	2.2×10^{-2}
	Utility		BNL	
			Before DELETE	After DELETE
2. 3-train plant with Westinghouse NSSS*				
a) LMFW	6.3×10^{-6}		2.6×10^{-5}	2.2×10^{-5}
b) LOOP	2.6×10^{-5}		1.2×10^{-4}	1.0×10^{-4}
c) LOAC	1.0×10^{-2}		3.2×10^{-2}	3.2×10^{-2}
	Utility		BNL	
	Before Design Changes		Before Design Changes	After Design Changes
3. 2-train plant with a startup pump and a Westinghouse NSSS ≠				
a) LMFW	2.1×10^{-5}		4.5×10^{-5}	2.0×10^{-5}
b) LOOP	5.2×10^{-5}		1.8×10^{-4}	8.6×10^{-5}
c) LOAC	2.1×10^{-2}		2.3×10^{-2}	2.3×10^{-2}

*The utility applied data for maintenance unavailabilities which were substantially lower than than prescribed in NUREG-0611.
≠The unacceptably high BNL results caused the utility to clarify and alter its design.

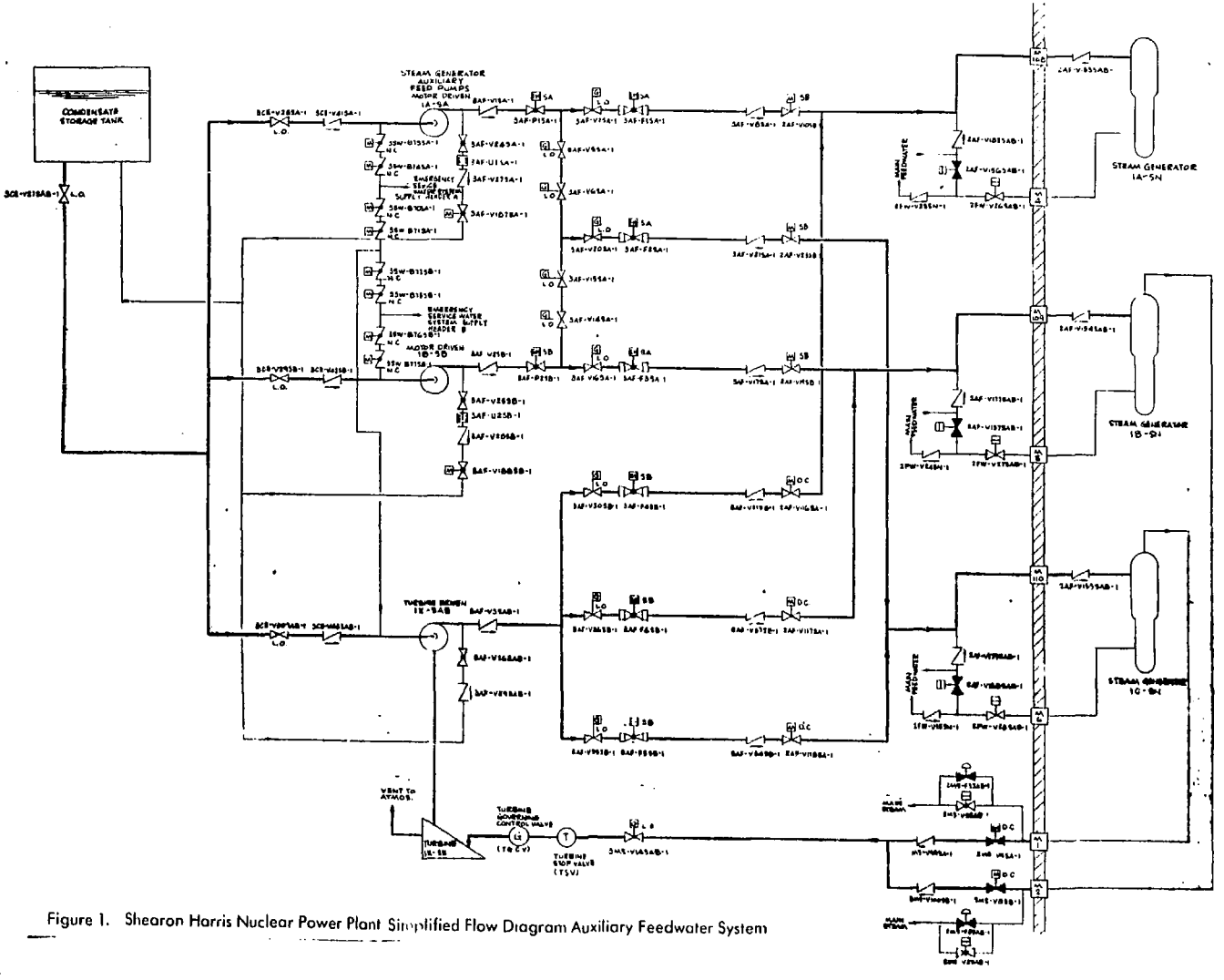

Figure 1. Shearon Harris Nuclear Power Plant Simplified Flow Diagram Auxiliary Feedwater System