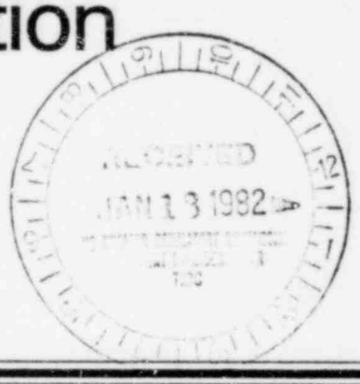
NUREG/CR-2322
SAND81-1943

Palo Verde Nuclear Generating Station Units 1, 2, and 3 Auxiliary Feedwater System Reliability Study Evaluation



Prepared by B. J. Roscoe

Sandia National Laboratories

Prepared for
U.S. Nuclear Regulatory
Commission

H003
s
0/1

NUREG/CR-2322
SAND81-1943

Palo Verde Nuclear Generating Station Units 1, 2, and 3 Auxiliary Feedwater System Reliability Study Evaluation

Manuscript Completed: July 1981
Date Published: December 1981

Prepared by
B. J. Roscoe

Sandia National Laboratories
Albuquerque, NM 87185

Prepared for
Division of Safety Technology
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN A1121

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 1717 H Street., N.W.
   Washington, DC 20555
2. The NRC/GPO Sales Program, U.S. Nuclear Regulatory Commission,
   Washington, DC 20555
3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports, vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the NRC/GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, transactions, and codes and standards. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free upon written request to the Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

ABSTRACT

The purpose of this report is to present the results of the review of the Auxiliary Feedwater System Reliability Analysis for the Palo Verde Nuclear Generating Station Units 1, 2 and 3.

Acknowledgement

The author appreciates the comments on the drafts provided by Jack W. Hickman of Sandia National Laboratories.

This report has extracted freely from the referenced documents.

Table of Contents

Table of Contents (Cont'd)

List of Figures

Summary and Conclusions

The accident at Three Mile Island resulted in many studies which outlined the events leading to the accident as well as those following. One of the important safety systems involved in the mitigation of such accidents was determined to be the Auxiliary Feedwater System. Each operating plant's Auxiliary Feedwater System was studied and analyzed. The results were reported in NUREG-0635[1]. The licensee of each non-operating plant was instructed[2] to perform a reliability analysis of his Auxiliary Feedwater System for three transient conditions involving loss of main feedwater in a manner similar to the study made by NUREG-0635 prior to their obtaining an operating license. Arizona Public Service Company, as Project Manager and Operating Agent for the Palo Verde Nuclear Generating Station Units 1, 2 and 3 submitted a reliability report[3] to the U.S. Nuclear Regulatory Commission (NRC) in February 1981. This report was reviewed by Sandia National Laboratories. The following conclusions resulted from the review:

1. Arizona Public Service Company has satisfactorily complied with the requirement to make a reliability study of their Auxiliary Feedwater System.
2. The Auxiliary Feedwater System AFWS has medium reliability relative to the reliability of Auxiliary Feedwater Systems of operating plants for the first case event, loss of Main Feedwater with Offsite Power Available. Quantitatively, the unavailability of the system is approximately 1.3×10^{-4} per demand. Qualitatively, the system is automatically initiated,

highly redundant, and has no observed single point vulnerabilities. Failure on demand is dominated by failure to properly align the system following test or maintenance. The utility has agreed to provide a position indication in the control room on the pump-test bypass valves and to have a second operator check manual valve positions following any realignment. Inclusion of these items places the system in the high reliability group. The unavailability for the second case event, Loss of Main Feedwater and Loss of Offsite Power, is approximately 1.4×10^{-4} per demand, which places the AFWS reliability in the medium range. This result (median value used in WASH-1400) in Case 2 assumes a diesel generator failure probability of .04 (median value used in WASH-1400). Failure on demand is dominated by failure to properly align the system following test or maintenance. Inclusion of the two features to assure proper alignment mentioned in Case 1 places the system in the high reliability group. The unavailability for the third case event, Loss of Main Feedwater and Loss of AHAC, is 1×10^{-2}, which places the reliability in the medium-to-high range. The turbine driven pump train has no identifiable ac power dependencies and is automatically actuated. Failure on demand is dominated by test and maintenance outage.

1. Introduction

The results of many studies pertaining to the Three Mile Island Nuclear Power Plant accident conclude that a properly functioning Auxiliary Feedwater System (AFWS) is of prime importance in the mitigation of such accidents. Therefore, a letter dated March 10, 1980[2], stating U.S. Nuclear Regulatory Commission (NRC) requirements regarding the AFWS, was sent to all operating license applicants with a Nuclear Steam Supply System (NSSS) designed by Westinghouse or Combustion Engineering.

Arizona Public Service Company (APS) as Project Manager and Operating Agent for the Palo Verde Nuclear Generating Station (PVNGS) Units 1, 2 and 3, which has a Combustion Engineering designed NSSS, provided a response in the form of a reliability analysis[3] which was prepared for them by Bechtel Power Corporation.

The analysis was received by SNL for review on 27 March, 1981.

The analysis makes a study of the failure of the AFWS to supply sufficient flow to either of two steam generators (SG).

The method of analysis consists of the construction and evaluation of fault trees. It takes into account active component failures, single passive failures, component outage due to test and maintenance, human errors, and common cause failures.

1.1 Scope and Level of Effort

This project undertakes a review of those portions of the reliability analysis which (1) satisfy requirement (b) of the letter which states, "perform a reliability evaluation similar in method to that described in Enclosure 1 (NUREG-0635) that was performed for operating plants and submit it for staff review," and (2) provide answers to the short and long-term recommendations of NUREG-0635 in response to requirement (c) in the letter.

The review was conducted according to a Schedule 189[4] which was submitted by SNL to NRC.

Sandia National Laboratories' review addressed the following issues:

(1) Mode of AFWS initiation

(2) System control following initiation

(3) Test and maintenance procedure and unavailability of AFWS

(4) Potential common mode factors in the AFWS

(5) Adequacy of emergency procedures for the operation and initiation

(6) Adequacy of power sources and separation of power sources

(7) Availability of alternate water sources

(8) Adherence to methodology and data presented in NUREG-0635

(9) Search for single failure points

1.2 Specific Review

SNL reviewed the reliability analysis[3] submitted by APS. Particular attention was directed toward determining that the analysis addressed in depth the reliability of the AFWS when subjected to three transient cases (1) Loss of Main Feedwater (LMF), (2) Loss of Main Feedwater/Loss of Offsite Power (LMF/LOSP) and (3) Loss of Main Feedwater/Loss of all AC Power (LMF/LAC). Also the methods used in NUREG-0635 were compared to those used in the analysis. The specific findings are presented in Sections 3, 4 and 5.

2. AFWS Configuration

The main function of the AFWS is to provide an independent means of supplying feedwater to the steam generators in addition to the main feedwater system. Another important function is to provide a sufficient supply of feedwater to permit the plant to operate at hot standby for eight hours followed by an orderly plant cooldown, at a rate not to exceed 75°F/hr, to the point where the shutdown cooling system may be initiated.

The AFWS consists of one safety-related Seismic Category I motor-driven pump (MDP), one safety-related Seismic Category I steam turbine-driven pump (TDP), one non-safety related non-Seismic Category I motor-driven pump, associated piping, controls, and instrumentation. Figure 1 shows the simplified piping and flow diagram of the system. The non-safety-related motor-driven pump will accrue the most duty because it is used for startup, hot standby, and normal shutdown operations.

The primary source of auxiliary feedwater is the Seismic Category I condensate storage tank (CST). A minimum capacity of 300,000 gallons is required by the AFWS to perform it's functions. During emergency shutdown conditions 330,000 gallons are available in the CST. This extra margin, though not required, enables an orderly cooldown of the reactor cooling system. The secondary or backup source of auxiliary feedwater is the reactor makeup water tank. It has a maximum capacity of 480,000 gallons.

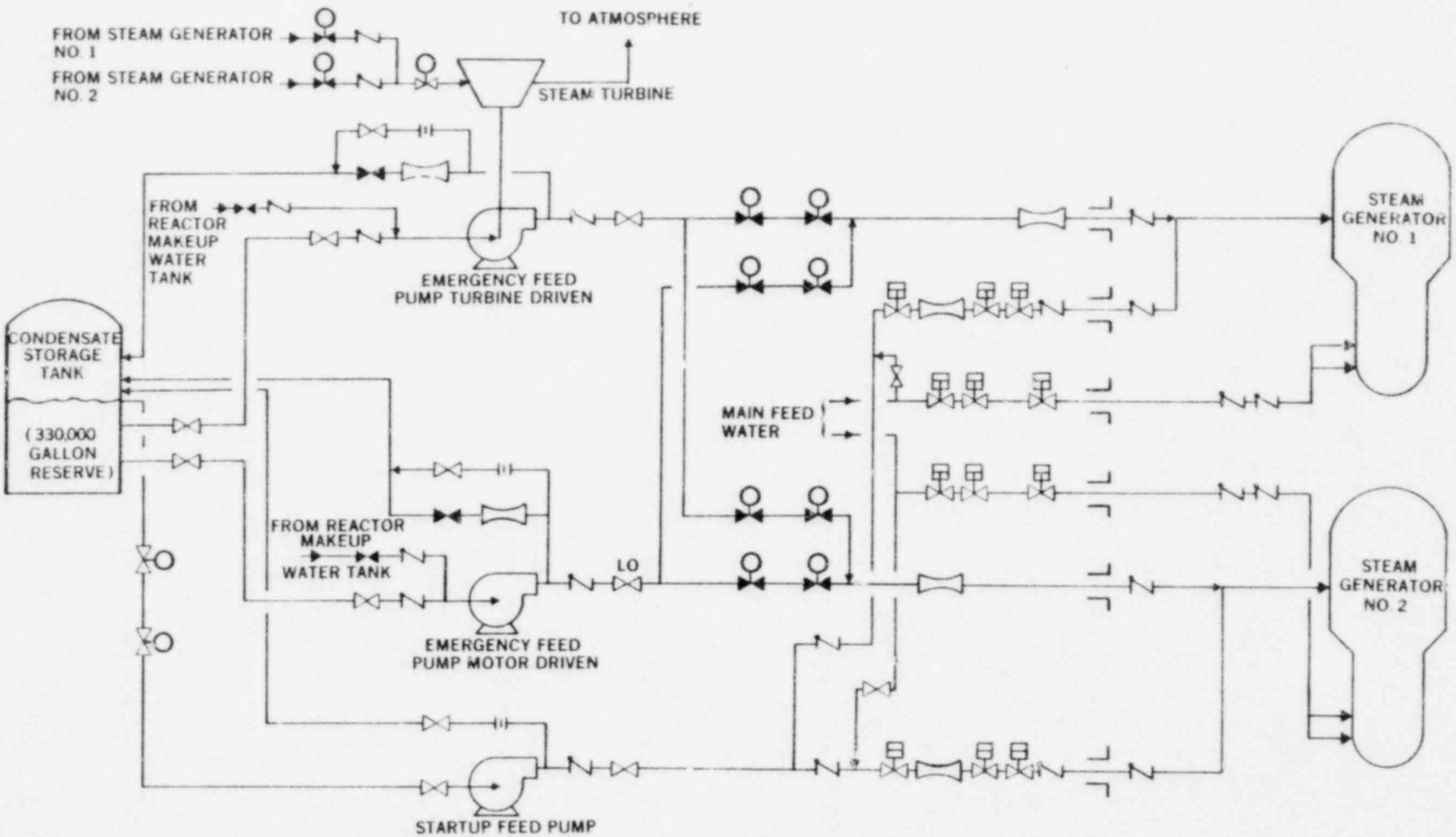


FIGURE 1 AUXILIARY FEEDWATER SYSTEM

The safety-related MDP and its motor-operated valves receive Class 1E power from either onsite or offsite power sources. In the event of a loss of offsite power, power is supplied to this MDP and its valves and controls by its emergency standby diesel generator. The loading of the emergency bus is sequential and automatic.

The TDP is supplied with steam from the main steam lines of either steam generator upstream of the main steam isolation valves. The power and controls for the valves associated with this pump receive power from the Class 1E dc buses A and C.

The two safety-related AFWS pumps are separated by a physical barrier. Piping and components are located, separated, or protected to preclude damage to each from common missile and environmental effects.

The emergency feedwater trains of the AFWS are able to withstand, and remain operable, during and after a safe shutdown earthquake.

2.1 System Description

The emergency feedwater pumps operate automatically upon receipt of an Auxiliary Feedwater Actuation Signal (AFAS) under the following emergency conditions:

- o Main steam line break
- o Loss of main feedwater
- o Loss of offsite power
- o Loss of all offsite and onsite ac power (TDP only)

Each emergency pump is capable of supplying 875 gpm into the steam generators at a pressure equal to the accumulation pressure of the lowest safety relief valve. Each emergency pump is also capable of supplying feedwater at steam generator pressures down to 135 psia. Low-pressure alarms are provided at each motor-driven pump discharge to preclude the possibility of pump runout and damage.

The emergency feedwater pumps are capable of delivering flow to the steam generators automatically upon receipt of an AFAS within the following criteria:

- o Within 10 seconds when offsite power is available.
- o Within 45 seconds when offsite ac power is not available (Diesel speed-up time).
- o After initiation of auxiliary feedwater flow there will be no decrease in the flow rate for any reason, other than as a result of the normal operation of the auxiliary feedwater controls, that will result in an effective loss of more than 15 seconds of full auxiliary feedwater flow (i.e., 875 gpm).

Initially, steam generator level is maintained automatically after initiation of an AFAS signal. After conditions stabilize, the operator has the capability of manually controlling the auxiliary feedwater flow for continuous feed to the steam generators as desired.

Signals from the AFAS automatically shut all isolation valves, and open the valves to the downcomer nozzles of the intact steam generator(s). The non-safety-related motor driven pump is started manually and its associated valves are opened manually from the control room.

A minimum flow-rate path is provided for each pump. Approximately 13% of the pump capacity is recirculated back to the condensate storage tank whenever a pump is operating. The minimum flow-rate line is provided to prevent pump over-heating in the event the pump discharge line is shut off. If a break is postulated to occur in the recirculation line downstream of the flow restriction orifice, system operation is not affected. The pump still delivers required flow to the steam generators. The water inventory of the condensate storage tank has been calculated to include the possibility of a 13% flow water loss through the recirculation line while maintaining a sufficient quantity of water to provide the required cooling. Recirculation lines to the CST are also provided downstream of the pumps to allow for full flow pump testing.

The motor-driven pump is powered from a separate engineered safety features (ESF) bus which is powered by the Train B diesel generator. The steam turbine-driven pump's associated valving is powered from the battery-backed essential dc bus A and C. The turbine for this pump is supplied with steam from either of the steam generators. The turbine controls are also powered from the dc bus A. For emergency operation, normal flow is from the condensate storage tank to both the safety-related MDP and to the TDP. An alternative supply of water is provided by local manual cross connections to the reactor makeup water tank.

The system, in conjunction with the main feedwater system, is designed to prevent waterhammer transients of water slugs that could result from vapor bubble collapse in the steam generator ring headers, valve closure, pump starts, and transfers.

Auxiliary feedwater control is normally from the control room, but instrumentation is provided for operation from the remote shutdown station in the unlikely event that the control room must be evacuated.

For normal (non-emergency) AFWS operation the non-safety-related pump, located in the turbine building, is employed.

One manually operated auxiliary feedwater path to the steam generators is provided for the non-safety-related motor-driven AFWS pump through the main feedwater header.

At a reactor coolant temperature of 350°F, the shutdown cooling system is placed in operation. The AFWS duty cycle is then completed and it is returned to standby status.

2.2 AFWS Support Systems

2.2.1 Power Sources

The active components of the AFWS are dependent upon diverse sources of electrical power. Lube oil and cooling subsystems are supplied power from the same source as the primary component. All valves and controls in the same train are similarly matched to the same power source as its pump, and key devices can be manually or locally actuated as well. Four independent transmission lines supply the offsite power, and two dedicated diesel generators back up the onsite Class 1E power buses. Each diesel generator may supply power to only one MDP by design.

2.2.2 Alternate Water Sources

There is a backup water supply source from the reactor makeup water tank. Up to 480,000 gallons of demineralized water can be made available to the AFWS suction cross-tie by means of a hand valve in the chemical and volume control system, then through 8-inch

piping to the safety-related motor-driven pump and to the turbine-driven pump.

2.2.3 Steam Availability

Steam to the turbine pump is provided by either steam generator from a point upstream of the main steam isolation valves (MSIVs). No automatically actuated valves are located upstream of the MSIVs except as required for supply to the steam driven emergency feedwater pump. Provisions are made to prevent blowdown of both steam generators through the emergency feedwater supply headers in the event of a steam line break. The TDP control system and its associated power operated valves are supplied by the Class 1E DC Power System.

2.2.4 Instrumentation and Controls

Control room instrumentation includes steam generator level controls and hand switches plus position indicators for all power operated valves.

Control logic for the AFWS is a manually overridable automatic two-of-four input signal system which is part of the Engineered Safety Features Actuation System (ESFAS). Steam generator pressure and water level are the monitored variables for automatic protective action.

The following main control room monitors are provided for purposes of AFWS control:

- o System trip status light.
- o Discharge pressure of each AFWS pump.
- o Auxiliary feedwater flow to each steam generator.
- o Two status lights for each regulator valve.
- o RPM of the turbine (pump driver).
- o Status lights for all motor operated valves.

2.2.5 Initiation Signals for Automatic Operation

The AFAS performs the following functions as intended by design:

A. Start the safety-related, motor-driven auxiliary feedwater pump whenever an AFAS occurs for either steam generator.

B. Open the steam supply valving to start the steam turbine driver whenever an AFAS occurs for either steam generator.

C. Determine whether a steam generator is intact in the event of a secondary system break.

D. Open the auxiliary feedwater regulating valves to the intact steam generator using the trip channel logic. The same logic is used to provide a closing signal, which can be overridden by the operators, to the auxiliary feedwater valves to a non-intact steam generator to prevent flow to that generator.

E. Close the steam generator blowdown line isolation valves whenever an AFAS occurs for either steam generator.

F. Prevent a high water level condition in the intact steam generator(s) by closing the auxiliary feedwater regulating valves when the level is reestablished above the low level trip setpoint. The valve logic is not latched in the actuated state in order that this control can be accomplished. When the level and pressure conditions for valve opening are again met, the valves are automatically reopened.

G. Start the diesel generators whenever an AFAS occurs for either steam generator.

H. An AFAS aligns the AFWS regulating and isolation valves to feed the intact steam generator(s). Once the steam generator level is restored, the pumps continue to operate, but the regulating and isolation valves close. The valves continue to cycle with steam generator level fluctuation. The steam generator level will be manually stabilized to avoid undue cycling of the regulating valves.

The system is designed such that loss of electric power to two of the four like channels in the measurement channels, or initiating logic, or to the selective two-out-of-four actuating logic will actuate the AFWS.

Manual control of the AFWS is provided by means of hand controllers on the main control panel. The operator may override the automatic system under all operating and accident conditions by controlling the AFWS regulating valves from the main control room.

2.2.6 Testing

The AFWS pumps are capable of being tested while the plant is in normal operation. A recirculation and full flow test line to the condensate storage tank enables the pumps to be operationally tested. Control room discharge pressure and local flow indicators are provided to monitor pump performance.

Containment isolation valves can be tested during normal plant operation. However, by technical specification, these valves will be tested only during refueling shutdown.

2.2.7 Technical Specifications

Technical Specifications require the availability of 300,000 gallons of water in the condensate storage tank for AFWS use. Water volumes below 530,000 gallons, 330,000 gallons and 20,000 gallons are alarmed and annunciated in the control room.

A maximum of 72 hours out of service is allowed for maintenance or repair of a safety-related pump while the reactor is critical. If that time is exceeded the reactor must be put in hot shutdown within the next 12 hours.

Surveillance Requirements

1) Each emergency feedwater pump shall be demonstrated operable:

   A. At least once per 30 days by:

      (1) Verifying turbine driven pump develops discharge pressure of $\geq$ 1260 psig at flow of $\geq$ 987 gpm when the secondary steam supply pressure is greater than 1035 psig.

      (2) Verifying each valve (manual, power operated or automatic) in the flow path that is not locked, sealed, or otherwise secured in position, is in correct position.

   B. At least once per 18 months during shutdown by:

      (1) Verifying each automatic valve in the flow path actuates to its correct position on MSIS and EFAS test signals.

      (2) Verifying motor driven pump starts automatically upon receipt of an EFAS test signal.

The condensate storage tank shall be demonstrated operable at least once per 12 hours by verifying the contained water volume is within its limits when the tank is the supply source for the emergency feedwater pumps.

The applicable alternative service water system (reactor makeup water tank is the alternate for PVNGS) shall be demonstrated operable at least once per 12 hours by verifying that at least one service water loop is operating and that the service water system - emergency feedwater system isolation valves are either open or operable whenever the service water system is the supply source for the emergency feedwater pumps.

3. Discussion

3.1 Mode of AFWS Initiation

The emergency pumps operate automatically upon receipt of an actuation signal. This signal is present under the following emergency conditions: main steam line break, loss of main feedwater, loss of offsite power, loss of all offsite and onsite ac power.

3.2 System Control Following Initiation

After automatic initiation of the AFWS, flow is automatically controlled by adjustment of the discharge control valves to control the level in the steam generators. As conditions permit, the operator has the capability of manually controlling flow for continuous feed to the steam generators. When the reactor coolant condition is reduced to 350°F the RHRS is placed into service and the AFWS taken out of service.

3.3 Test and Maintenance Procedures and Unavailability

The technical specifications require that all valves be given in service tests and inspections in accordance with the ASME Boiler and Pressure Vessel Code (Section XI and applicable Addenda) for Safety class 1, 2, and 3 components. Also every 31 days there are

(1) pump discharge pressure and flow tests, (2) non-automatic valve position verification test, and (3) automatic valve position verification when the AFWS system is in automatic control. The pumps and system are available on demand during all tests. During shutdown the automatic starting of each pump and the functioning of the automatic valves from closed to full open in the suction line of each AFWS pump from the CST are checked. There are no coincident tests or maintenance of components within the AFWS. There was evidence that the actual test and maintenance procedures were reviewed and considered in the reliability analysis.

3.4 Adequacy of Emergency Procedures

The emergency operation procedures will incorporate the necessary operator action to protect the AFWS pumps if the primary source is lost. This will involve realignment to the backup source, the Reactor Makeup Water Tank (RMWT), when the primary source, the condensate storage tank, is lost.

When the primary source is being depleted, the emergency operating procedure will insure that the RMWT is lined up as needed to supply the AFWS pumps when the CST is at its minimum allowable level.

The procedures are inadequate with respect to "Short-Term Generic Recommendation GS-4" in that there is no criteria to inform the

operator when, and in what order, the transfer to alternate water sources should take place.

3.5 Adequacy of Power Sources and Separation of Power Sources

The active components in each train are supplied with diverse sources of electrical power. Motor-operated valves, controls, lube oil, and cooling systems in a train are supplied from the same independent electrical source as the pump. Four independent transmission lines supply offsite power and two dedicated diesel generators backup onsite class 1E power buses. The TDP is supplied with steam from either of two steam generators. The TDP is not dependent upon offsite or diesel ac power. Redundant power sources enhance system reliability as does the separation of these power sources which eliminates many common cause failure events.

3.6 Availability of Alternate Water Sources

Water of steam generator quality is available from the reactor makeup water tank. This tank has a capacity of 480,000 gallons and can be manually tied into the system in the event a low level condition is reached in the CST. An alarm on the CST level allows an operator thirty minutes to switch to the alternate source.

3.7 Potential Common Mode Failure

Common cause analysis was included in the reliability analysis. Qualitative analysis was performed to identify potential sources of common cause failures while quantitative analysis was done to indicate the limited effect that increased redundancy can have on the reliability of a system.

The first step in the qualitative analysis was identification of common or similar hardware, test, maintenance, human actions or physical links between redundant trains. An in-house computer code was developed by Bechtel to indicate the number and type of commonalities (such as, thermal, radiation, grit, chemical, etc.) that exist among the components of the redundant trains. The greater the commonality, the greater the potential for common cause may exist. There were twenty-five possible categories of commonality but the number of actual common categories found were six. All sets of components with six commonalities were selected (there were fifty-two) and these sets were compared to the minimal cut sets to identify sources of common mode failure. No serious potential for common cause was found using this approach.

The β-factor method was used to quantitatively estimate the effect of common cause failures. The β-factor method assumes that a fraction of the operationally independent failure

probabilities of one loop (Q_{loop}) of a redundant system will result in the loss of all redundant loops in that system. The analysis used a β-factor of $\beta = 2.7 \times 10^{-2}$. This is a mean value based on an assumed range of 10^{-1} to 10^{-3} where the log normal distribution is assumed.

The common cause failure probability, Q_{cc}, for a redundant system can be approximated by the failure probability of one loop of a redundant system, Q_{loop}, times β added to the independent failures.

In general, the β-factor approach to common cause failure estimates shows its greatest impact on system reliability for highly redundant and simultaneous operating systems to the extent that adding more redundancy than is necessary to prevent single point failures is generally not warranted if β-factor common cause methodology is assumed.

For this analysis, the following assumptions were made:

1. The cross-over MOVs, check valves, DC/vital instrument buses, AFAS signal, electric pump and buses, human error, and the diesel generators were identical or similar and thus subject to the common cause β-factor.

2. The turbine drive and electric drive pumps were diverse and not subject to the common cause β-factor.

3. The inter-train common cause failures were considered.

The common cause failure probability contributions to the AFWS were calculated using the β-factor method and added to the independent failure probabilities. The result was that the reliability of the AFWS was relatively poor for all three transients. The unavailability for the first, second and third transients was 1.1×10^{-3}, 1.6×10^{-3}, and 6.2×10^{-2} per demand, respectively. These poor results are due to the utilization of the β-factor method in the analysis. Since this method is not part of the methodology of NUREG-0635, these quantitative results cannot logically be compared to the results of NUREG-0635.

3.8 Application of Data Presented in NUREG-0635

Quantitative techniques are used in the reliability analysis which are different and more complex than those described in NUREG-0635. The analysis includes error bounds on the results, incorporates the β-factor method for common cause failures and gives a more conservative treatment of human error. The data given in NUREG-0635 are not applied directly, but are assumed to be median values of a lognormal distribution from which mean values and variances are calculated. The calculated means are then used to quantify the analysis which is based on fault tree methods. As a result of the different and more complex analysis used by Bechtel, the quantitative unavailability of the AFWS is more than an order of magnitude lower, for each case, in comparison with unavailability of the AFWSs of operating plants. However, these results cannot be justifiably compared

because the latter were obtained from a simplified, less conservative analysis.

3.9 Search for Single Failure Points

There were no single active component failure points associated with Case 1, LMF, or Case 2, LMF/LOSP. For Case 3, LMF/LAC, there were many single failure points since Case 3 describes a single channel system. The condensate storage tank and the piping and valves connected to the tank have the potential to be passive single component failure points if any of these components were to have a severe leak or rupture. The failure probability of such an event was estimated to be negligible.

Any single failure point has the potential for a major effect on the reliability of a redundant system and if any are found, they should be evaluated for their likelihood of occurrence and compensated if they are not sufficiently rare.

3.10 Human Factors/Errors

Human factors/errors were considered where appropriate in the fault tree. Automation is a major factor in decreasing the effect on reliability of these types of events.

Human factors/errors were taken into account by APS and combined into the second level fault tree (i.e., one level below the top

event) along with hardware independent failures and test and maintenance failures. Three categories of human errors appear as basic events in this part of the fault tree. These are "valve closed as a result of maintenance," "valve open as a result of test," and "failure to close or open valve during operation." These types of errors, in particular leaving the pump recirculation valve open after a full flow pump test and leaving the pump discharge manual valve closed following maintenance on a pump, account for the largest contribution to unavailability. Automation is a major factor in decreasing the effects of human error on unavailability.

3.11 NUREG-0635 Recommendations, Long- and Short-Term

Reference 2 of this report contained Enclosure 1 which stated a number of short-term generic, additional short-term, and long-term generic recommendations. The reponse of APS to these recommendations are contained in a letter[5] to Mr. Harold R. Denton, dated May 1, 1981. The issues have been satisfactorily resolved. Some changes in the AFWS which improve reliability occurred as a result of implementing these recommendations and those of the reliability analysis. These changes are discussed in Section 4.

4. Major Contributions to Unreliability

A number of recommendations for changes in the AFWS were developed from the NUREG-0635 generic recommendations and the reliability evaluation of PVNGS AFWS. The recommendations and corresponding responses from APS are the following:

RECOMMENDATION #1

Provide the capability to supply the start-up auxiliary feedwater pump from the train A diesel generator.

Response

The design has been modified to incorporate this recommendation.

RECOMMENDATION #2

Provide position indication in the control room for the pump test bypass valves.

Response

The design has been modified to incorporate the recommendation.

RECOMMENDATION #3

Provide power to the suction valves for the start-up auxiliary feedwater pump from the train A diesel generator.

Response

The design has been modified to incorporate the recommendation.

RECOMMENDATION #4

Perform a total system test once every 18 months.

Response

PVNGS will adopt Technical Specifications to assure that, prior to plant start-up following an extended cold shutdown, a flow test will be performed to verify the normal flow path from the primary AFWS water source to the steam generators.

RECOMMENDATION #5

Perform testing on different shifts.

Response

Having different operators perform surveillance tests on the AFWS will not be required at PVNGS. Surveillance tests are of a frequency and complexity such that the operator will be required to use written procedures to conduct the tests. These procedures will contain appropriate sign-offs and checklists to insure that the testing is conducted in accordance with the procedure.

Maintenance or testing procedures which require realignment of valves from the normal position will incorporate a valve line-up checklist as part of the restoration.

The above changes are taken into account in the final evaluation of the Palo Verde AFWS system.

The results given in the report, based upon NUREG-0635 methods, are high for each transient, but they are derived from qualitative analysis. During the course of the review, however, a quantitative analysis based upon NUREG-0635 was performed by Sandia.

A summary of the Sandia reliability analysis and review for the three events are given as follows:

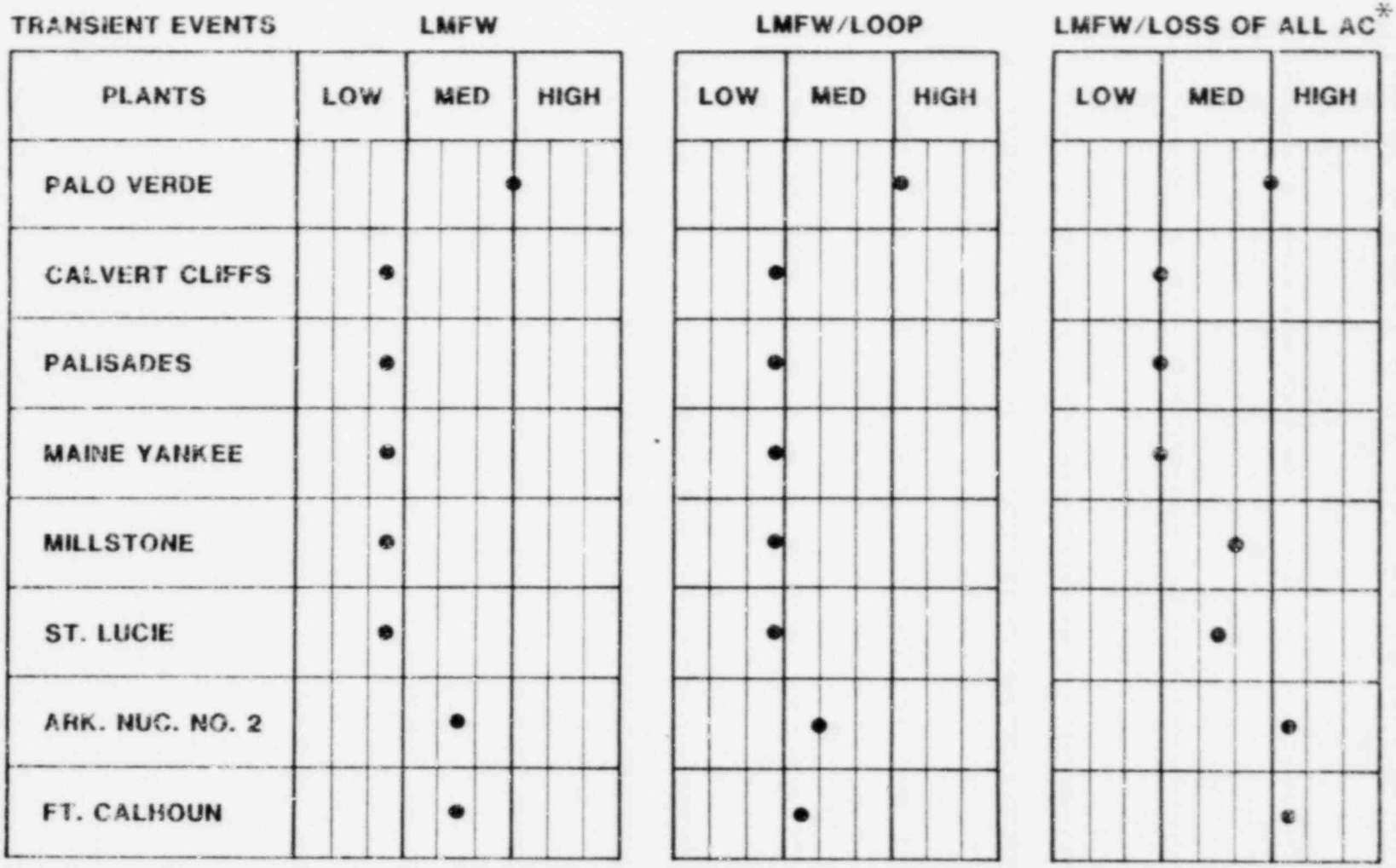
1. Loss of Main Feedwater with Offsite Power Available -- No single failures that would result in insufficient auxiliary feedwater flow were identified. The analysis indicated that the largest unavailability was due to human error. The applicable human errors are inadvertently leaving the pump recirculation valve open after a full flow pump test, and leaving the pump discharge manual valve closed following maintenance on the pump. The unavailability of the AFWS for Case 1 is 1.3×10^{-4} per demand, which places this system in the medium reliability group relative to operating PWRs. Two recommendations that improve reliability for this transient have already been accepted by the utility. These are to provide position indication in the control room on pump-test bypass valves and to have a second operator check manual valve positions following any realignment. Inclusion of these recommendations places the AFWS in the high reliability group.

2. Loss of Main Feedwater and Loss of Offsite AC -- If the diesels have high reliability, the system reliability is approximately the same as Case 1 above. If the diesels have low reliability, the system reliability approaches the

reliability of Case 3 below. For diesel generator failure probability as high as .04 (given as a median number in WASH-1400), the unavailability of the AFWS is 1.4×10^{-4} per demand, which places this system in the medium reliability group relative to operating PWRs. The dominant failure for this case is the same as for Case 1. Inclusion of the two recommendations in Case 1 places the AFWS in the high reliability group for this transient.

3. Loss of Main Feedwater and Loss of All AC -- If all AC power is lost, there is only the turbine driven pump (TDP) available. In this case, the dominant failure is the TDP being out of service due to test or maintenance. The unavailability is approximately 1×10^{-2} per demand, which places this system in the medium-to-high reliability group relative to operating PWRs.

These conclusions are plotted in Figure 2 along with the operating plant ratings which were derived from NUREG-0635.



* SCALE FOR THIS EVENT IS DIFFERENT FROM THE OTHER TWO SCALES

RELIABILITY CHARACTERIZATONS FOR AFWS DESIGNS IN PLANTS USING THE COMBUSTION ENGINEERING NSSS AND PALO VERDE

FIGURE 2

5. Conclusions

It is concluded on the basis of this review that APS has completed requirement (b) of the March 10, 1980 letter. The method of analysis consists of the construction and evaluation of fault trees. As indicated in NUREG-0635, the second level of the system fault tree contains common failures affecting both trains, independent train failures, and failure due to test and maintenance.

The AFWS of the PVNGS, Units 1, 2, and 3, has medium reliability relative to the reliability of the AFWSs of operating plants for Case 1, loss of main feedwater. Quantitatively, the unavailability of the system was found to be approximately 1.3×10^{-4} per demand. This result is based upon application of data presented in NUREG-0635. Qualitatively, the system is automatically initiated, highly redundant, and has no observed single point vulnerabilities. The active components in each train are supplied with diverse sources of electrical power. The alternate water source is adequate and the CST has a low level alarm. Failure on demand is dominated by failure to properly align the system following test or maintenance. The utility has agreed to provide a position indication in the control room on the pump-test bypass valves and to have a second operator check manual valve positions following any realignment. Inclusion of these items places the AFWS in the high reliability group. The unavailability for Case 2 is

approximately 1.4×10^{-4} per demand, which places the AFWS reliability in the medium range. This result obtains in Case 2 for an assumed diesel generator failure probability of .04 for each diesel generator. This value of failure probably is high enough that there is little difference in the reliability of the AFWS between Cases 1 and 2. Failure on demand is dominated by failure to properly align the system following test or maintenance. Inclusion of the two items mentioned in Case 1 places the system in the high reliability group.

The unavailability for Case 3 is $1 \times 10^{-}$, which places the reliability in the medium-to-high range. In this case all ac power is lost and only the TDP is available. The dominant failure modes are single events. The TDP train has no identifiable ac power dependencies and is automatically actuated. Failure on demand is dominated by test and maintenance outage.

6. Glossary of Terms

AC	Alternating Current
ac	alternating current
AFAS	Auxiliary Feedwater Actuation Signal
AFW	Auxiliary Feedwater
AFWS	Auxiliary Feedwater System
APS	Arizona Public Service Company
ASME	American Society of Mechanical Engineers
B/PV	Boiler and Pressure Vessel
CST	Condensate Storage Tank
DBE	Design Basis Earthquake
DC	Direct Current
dc	direct current
EAPS	Essential Auxiliary Power System
ESFAS	Engineered Safety Features Actuation System
FSAR	Final Safety Analysis Report
gpm	gallons per minute
IEEE	Institute of Electrical and Electronic Engineers
LAC	Loss of all AC power
LMF	Loss of Main Feedwater
LOCA	Loss of Coolant Accident
LOSP	Loss of Offsite Power
MDP	Motor Driven Pump
MSIS	Main Steam Isolaton Signal
MSIV	Main Steam Isolation Valve

Glossary of Terms (Cont'd)

NPSH	Net Positive Suction Head
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
NSWS	Nuclear Service Water System
psig	pounds per square inch gage
PVNGS	Palo Verde Nuclear Generating Station
RHRS	Residual Heat Removal System
RMWT	Reactor Makeup Water Tank
RPM	Revolutions Per Minute
SFP	Single Failure Point
SGBS	Steam Generator Blowdown System
SNL	Sandia National Laboratories
TDP	Turbine Driven Pump
V	Volt

7. References

1. NUREG-0635 "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Combustion Engineering Designed Operating Plants"; Office of Nuclear Reactor Regulation; U.S. Nuclear Regulatory Commission; NUREG-0635; January 1980.

2. Letter to all Pending Operating License Applicants of Nuclear Steam Supply Systems Designed by Westinghouse and Combustion Engineering from D. F. Ross. Jr., Acting Director Division of Project Management Office of Nuclear Reactor Regulation, Subject, Actions Required from Operating License Applicants of Nuclear Supply Systems Designed by Westinghouse and Combustion Engineering Resulting from the NRC Bulletins and Orders Task Force Review Regarding the Three Mile Island Unit 2 Accident, dated March 10, 1980.

3. "Palo Verde Nuclear Generating Station Auxiliary Feedwater System Reliability Analysis" Submitted under Docket Nos. STN-50-528/529/530 by Arizona Public Service; February 10, 1981.

4. Schedule 189 No A1121-0 Title, "Review of Auxiliary Feedwater System Reliability Evaluation Studies for Diablo Canyon I, McGuire 1, Summer 1, San Onofre 2, and Palo Verde" dated August 6, 1980.

5. Letter to Mr. Harold R. Denton, Director of NRR, from E. E. Van Brunt, Jr., APS Vice President, dated May 1, 1981, ANPP-17884-JMA/TFQ.

Distribution: SAND81-1943/NUREG/CR-2322

US Nuclear Regulatory Distribution Contractor (CDSI)
7300 Pearl Street
Bethesda, MD 20014
130 copies for AN
25 copies for NTIS

Author selected distribution - 1 copy
(List available from author.)

4400 A. W. Snyder
4412 J. W. Hickman (5)
4412 B. J. Roscoe (2)
8214 M. A. Pound
3141 L. J. Erickson (5)
3151 W. L. Garner (3)
For DOE/TIC (Unlimited Release)

NRC FORM 335 (7-77)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER (Assigned by DDC)
NUREG/CR-2322
SAND81-1943

4. TITLE AND SUBTITLE (Add Volume No., if appropriate)
Palo Verde Nuclear Generating Station Units 1, 2, and 3 Auxiliary Feedwater System Reliability Study Evaluation

2. (Leave blank)

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)
B.J. Roscoe

5. DATE REPORT COMPLETED
MONTH: July | YEAR: 1981

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Sandia National Laboratories
Albuquerque, NM 87185

DATE REPORT ISSUED
MONTH: December | YEAR: 1981

6. (Leave blank)

8. (Leave blank)

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Division of Safety Technology
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555

10. PROJECT/TASK/WORK UNIT NO.

11. CONTRACT NO.
NRC FIN A1121

13. TYPE OF REPORT

PERIOD COVERED (Inclusive dates)

15. SUPPLEMENTARY NOTES

14. (Leave blank)

16. ABSTRACT (200 words or less)

The purpose of this report is to present the results of the review of the Auxiliary Feedwater System Reliability Analysis for the Palo Verde Nuclear Generating Station Units 1, 2, and 3.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS (This report)
Unclassified

21. NO. OF PAGES

20. SECURITY CLASS (This page)
Unclassified

22. PRICE
$

NRC FORM 335 (7-77)