



NUREG/CR-1925
SAND81-0242

Diablo Canyon Nuclear Power Station Unit 1 Auxiliary Feedwater System Reliability Study Evaluation

Prepared by G. H. Bradley, Jr.

Sandia National Laboratories

Prepared for
U.S. Nuclear Regulatory
Commission

NOTICE

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, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Available from

GPO Sales Program
Division of Technical Information and Document Control
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Printed copy price: \$4.00

and

National Technical Information Service
Springfield, Virginia 22161

Diablo Canyon Nuclear Power Station Unit 1 Auxiliary Feedwater System Reliability Study Evaluation

Manuscript Completed: February 1981
Date Published: July 1981

Prepared by
G. H. Bradley, Jr.

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

ABSTRACT

The purpose of this report is to present the results of the review of the Reliability Analysis of the Diablo Canyon Auxiliary Feedwater System. The analysis was prepared for Pacific Gas and Electric Company, the licensee for Diablo Canyon, by Pickard, Lowe and Garrick, Inc.

Contents

	<u>Page</u>
Summary and Conclusions	1
Abbreviations	3
1. Introduction	4
1.1 Background	4
1.2 Review Activity	4
1.3 Content and Results of the Reliability Analysis	5
1.4 Scope and Level of SNL Effort	5
2. AFWS System Configuration	6
2.1 Mechanical System	6
2.2 Instrumentation and Controls	9
3. Discussion	
3.1 Mode of AFWS Initiation	10
3.2 System Control following initiation	12
3.3 Test and Maintenance Procedures and Unavailability	12
3.3.1 Procedures	12
3.3.2 Testing	16
3.3.3 Unavailability	17
3.3.4 Discussion of Failure Modes	17
3.4 Adequacy of Emergency Procedures	20
3.5 Adequacy of Power Sources and Separation of Power Sources	24

Contents (Cont'd)

	<u>Page</u>
3.6 Availability of Alternate Water Sources	24
3.7 Potential Common Mode Failures	24
3.8 Application of Data Presented in NUREG-0611	26
3.9 Search for Single Failure Points	26
3.10 Human Factors/Errors	26
3.11 NUREG-0611 Recommendation, long and short-term	27
3.11.1 Short Term Generic Recommendations	27
3.11.2 Additional Short Term Recommendations	38
3.11.3 Long Term Generic Recommendations	42
4. Major Contribution to Unreliability	45
5. Conclusions	49
6. References	52

List of Figures and Tables

<u>Figure</u>		<u>Page</u>
1	Diablo Canyon Auxiliary Feedwater System	7
2	Reliability Characterizations for AFWS Designs in Plants Using the Westinghouse NSSS	50

<u>Table</u>		<u>Page</u>
1	AFWS Instrumentation at Diablo Canyon	11
2	Dominant Contributors to Conditional Unavailability Case 1 - Loss of Main Feedwater	46
3	Dominant Contributors to Conditional Unavailability Case 2 - Loss of Main Feedwater and Loss of Offsite Power	47
4.	Dominant Contributors to Conditional Unavailability Case 3 - Loss of Main Feedwater and Loss of all ac power	48

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 (AFWS). Each operating plant's AFWS was studied and analyzed. The results for Westinghouse designed plants were reported in NUREG-0611. Prior to obtaining an operating license, the applicant for each non-operating plant is required to perform a reliability analysis of his AFWS in a manner similar to the study made in NUREG-0611. Pacific Gas and Electric Company (PG&E), the applicant for an operating license for the Diablo Canyon Nuclear Power Station submitted a reliability report to NRC in July 1980. This report was reviewed by Sandia National Laboratories (SNL). The following conclusions resulted from the review:

1. Compliance to Letter of March 10, 1980

PG&E has complied with requirement (b) of the letter which states:

"(b) perform a reliability revaluation similar in method to that described in Enclosure 1 that was performed for operating plants and submit it for staff review." Enclosure 1 to the letter of March 10th provides the applicable portions of NUREG-0611 which deal with the Auxiliary Feedwater Systems.

2. Major Contributions to Unreliability

The PG&E report adequately discussed the major contributors to unreliability for the three cases, (1) LMFW, Loss of Main Feedwater, (2) LMFW/

LOOP, Loss of Main Feedwater/Loss of offsite power, and (3) LMFW/LAC, Loss of Main Feedwater/Loss of all ac power. The major contributor in Case 1 and 2 is the failure or incorrect positioning of the Condensate Storage Tank (CST) outlet valve 1-671 combined with no operator action to trip the Auxiliary Feedwater (AFW) pumps. The valve, 1-671, is in the common pipe which provides water from the CST to all AFW pumps. The major contributors in Case 3 were the steam turbine and its supporting systems.

3. Method Used by PG&E

The method used by PG&E was in general agreement with the method used in NUREG-0611. All areas of the study were adequately addressed.

4. Final assessment by PG&E

The final assessment made by PG&E places Diablo Canyon at the high end of the range of reliability reported in NUREG-0611 for operating Westinghouse plants. Sandia is not in agreement with this assessment for Case 1 and 2 because of questionable recovery factors used to lower the failure assessment of critical basic events. Sandia concludes that for Case 1 and 2 the reliability should be in the medium range.

Abbreviations

ac	alternating current
AFW	Auxiliary Feedwater
AFWS	Auxiliary Feedwater System
AFWP	Auxiliary Feedwater Pump
ATWS	Anticipated Transient without Scram
CST	Condensate Storage Tank
dc	direct current
EOP	Emergency Operating Procedure
FCV	Flow Control Valve
FWST	Fire Water Storage Tank
LAC	Loss of all AC power
LCV	Level Control Valve
LMFW	Loss of Main Feedwater
LOOP	Loss of Offsite Power
MDP	Motor Driven Pump
MOV	Motor Operated Valve
NPSH	Net Positive Suction Head
NRC	Nuclear Regulatory Commission
PG&E	Pacific Gas and Electric Company
RWSR	Raw Water Storage Reservoir
SFP	Single Failure Point
SI	Safety Injection
SNL	Sandia National Laboratories
TDP	Turbine Driven Pump

Diablo Canyon Nuclear Power Station Unit 1
Auxiliary Feedwater System Reliability Study Evaluation

1. Introduction

1.1 Background

The results of many studies pertaining to the Three Mile Island Nuclear Power Station accident conclude that the proper functioning of the Auxiliary Feedwater System (AFWS) is of prime importance in the mitigation of such accidents. Therefore a letter dated March 10, 1980,¹ stating NRC's requirements regarding the AFWS was sent to all operating license applicants with Nuclear Steam Supply Systems designed by Westinghouse and Combustion Engineering.

The Pacific Gas and Electric Company (PG&E) San Francisco, California, the applicant for an operating license for the Diablo Canyon Nuclear Power Station Unit 1 which has a Westinghouse designed Nuclear Steam Supply System, provided a response in the form of a reliability analysis which was prepared for them by Pickard, Lowe and Garrick, Inc.² The analysis addressed requirement (b) of the letter which states, "perform a reliability evaluation similar in method to that described in Enclosure 1 (NUREG-0611)³ that was performed for operating plants and submit it for staff review."

1.2 Review Activity

This project undertakes a review of the reliability analysis² and the response⁴ of PG&E to requirement (c) of the letter¹ which states, "factor the recommendations of Enclosure 1 (NUREG-0611) into

your plant design." The review was conducted according to schedule 189 which was submitted by Sandia National Laboratories (SNL) to NRC.⁵

1.3 Content and Results of the Reliability Analysis

The reliability analysis was submitted to NRC in July 1980 and was received by SNL on September 1, 1980. Revision 3⁶ was submitted to NRC in September 1980 and was received by SNL on October 10, 1980. The analysis makes a detailed study of the failure of the AFWS to provide sufficient flow to any one of the four steam generators and compares the results obtained with those obtained for the operating plants studied in NUREG-0611. The analysis places Diablo Canyon Nuclear Power Station with those operating plants having high AFWS reliability.

1.4 Scope and Level of Effort

Initially SNL reviewed the reliability analysis² submitted by PG&E. Particular attention was directed toward determining that the analysis addressed in depth the reliability of AFWS when subjected to three transient cases (1) LMFW, Loss of Main Feedwater, (2) LMFW/LOOP, Loss of Main Feedwater and Loss of Offsite Power, and (3) LMFW/LAC, Loss of Main Feedwater and Loss of all ac power. Also the methods used in NUREG-0611 were compared to those used in the analysis. The specific findings are presented below in Sections 3, 4 and 5.

Comments and questions were recorded and submitted to NRC on the 16th of September. The questions were forwarded to PG&E by NRC. PG&E and its contractor, Pickard, Lowe and Garrick Inc., met with representatives from NRC and SNL on the 16th and 17th of October at Diablo Canyon Nuclear Station. At this meeting a review of the Diablo Canyon AFWS and the AFWS reliability analysis was given by Pickard, Lowe and Garrick, Inc. and a tour of the AFWS was conducted by PG&E. During the tour observations were made to facilitate the discussion period which followed. In the discussion period each of the 45 original questions was answered and discussed in detail. In addition 40 additional questions were answered. As a result of the questions a prompt and extensive revision⁶ was made to the preliminary issue of the reliability analysis. No exact verification of the numerical results were made; however, checks were made to assure us that the numbers reported were satisfactory.

2. AFWS System Configuration

2.1 Mechanical System

The AFWS consists of two motor-driven pumps and one turbine-driven pump as shown in Figure 1. Each motor-driven pump (490 gpm at 3000 feet) normally supplies two steam generators through electrohydraulic level control valves. The turbine-driven pump (930 gpm at 3000 feet) is normally lined up to supply all four steam generators through individual normally open motor-operated valves. The system can succeed in removing the decay heat from the core if sufficient

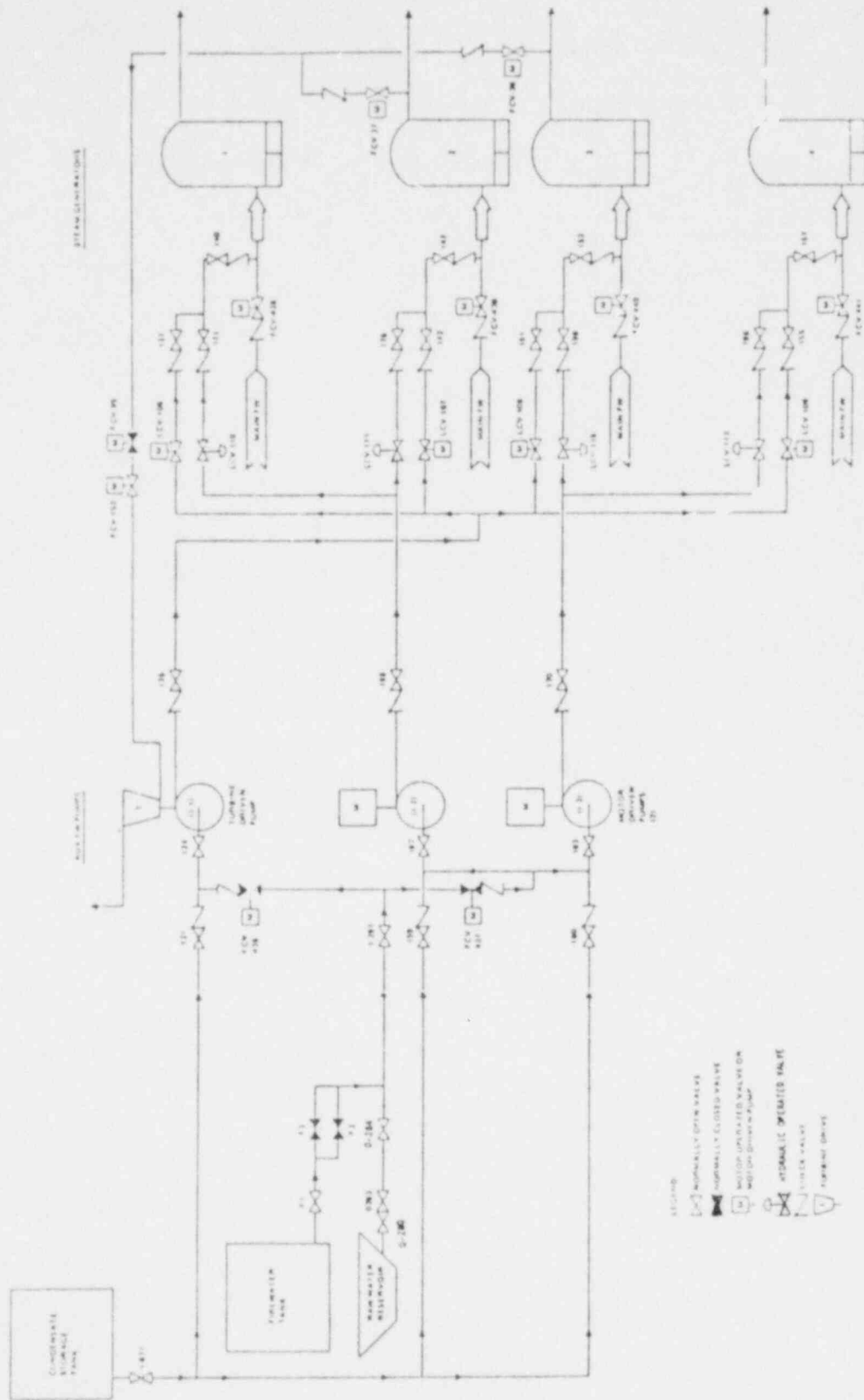


FIGURE 1. DIABLO CANYON AUXILIARY FEEDWATER SYSTEM

flow from any one pump (400 gpm) is delivered to any one steam generator. Natural circulation cooling for the core has been shown to be satisfactory to prevent core damage if there is sufficient water level on the secondary side of at least one steam generator and if the primary system retains sufficient water to keep the core covered even if the primary side contains water and steam mixture.⁷

The primary source of water for the AFWS is the Condensate Storage Tank (CST). This tank is Seismic Category I and is located adjacent to the Unit Auxiliary Building. The CST normally contains about 178,000 gallons which is enough to maintain the plant at hot standby for 8 hours after a reactor trip. The backup water source for the AFWS is the Fire Water Storage Tank (FWST). Operator action is required to manually align the FWST to the AFW pump backup suction header. An alternate backup supply of water is provided by the Raw Water Storage Reservoir (RWSR). This source is always aligned to the AFW pump backup suction header and is isolated in accordance with plant emergency operating procedure requirements before pump suction is shifted from the CST to the FWST.

The motor-driven pumps are powered from separate 4160 Vac vital buses. These vital buses are powered by separate emergency diesel generators. The turbine-driven pump receives steam from two of the four steam generators. The steam from each of the two steam generators passes

through a normally open motor-operated valve to a common turbine supply header. The turbine steam supply isolation valve, FCV-95, is normally closed and opens automatically in response to an actuation signal. This valve is presently ac powered but will be shifted to a dc supply before the plant is operated.

2.2 Instrumentation and Controls

The control of steam generator water level is dependent upon the pumps in service. The motor-operated flow control valves in the turbine driven pump discharge lines are controlled by separate three position switches in the main control room. The switches allow for opening, closing, or stopping the valves. To fully open or close these valves, the switch for an individual valve must be held in the open or close position. The individual switches are spring return to stop. These valves are normally in the full open position. The electro-hydraulic level control valves (LCVs) in the motor-driven pump discharge lines are normally in the full open position with their controllers set to AUTO. Automatic control of each LCV responds to the associated steam generator level. There is an overriding valve closure signal on low pump discharge pressure to protect the motor driven pumps from runout. The LCVs fail open on loss of power and will not respond to the steam generator level unless the associated auxiliary feedwater pumps are running.* A toggle switch is provided on the AFWS panel in the control room to bypass the pump-running interlock. The override switch permits valve closure for surveillance testing. None of the valves in the

*The LCVs on the turbine-driven AFW pump and all motor-operated valves in this system fail as-is on a loss of electric power.

auxiliary feedwater lines to the steam generators receive an automatic open signal in response to AFWS actuation.

The AFWS pumps and motor-operated valves may be operated from the Main Control Board or the Hot Shutdown Panel. Instrumentation available to the operator is presented in Table 1. This instrumentation allows for operator control of the system and aids in diagnosing problems in the system.

The motor-driven AFW pumps start automatically on steam generator low-low level in any one steam generator, on a Safety Injection (SI) signal, on auto trip of the main feed pumps, or on an associated vital bus transfer to diesel power. FCV-95 opens automatically to start the turbine-driven AFW pump on steam generator low-low level in any two steam generators or loss of power to the Reactor Coolant Pump buses (sensed by bus undervoltage devices).

3. Discussion

3.1 Mode of AFWS Initiation

The AFWS is initiated automatically. The motor-driven pumps (MDPs) will start on low-low level in any one steam generator, on a Safety Injection (SI) signal on auto trip of the main feed pumps, or on an associated vital bus transfer to diesel power. The Turbine-Driven Pump (TDP) is started by the automatic opening of FCV-95 on steam

TABLE 1 AFWs INSTRUMENTATION AT DIABLO CANYON

Indication	Comments
Auxiliary feedwater flow	One flow indicator per steam generator.
Steam generator water level	Wide range and narrow range for each steam generator, high and low level, also alarmed.
AFW pump discharge pressure	One per pump.
AFW pump suction pressure	Low pressure alarm only.
CSP water level	Low level also alarmed.
RWST water level	
Raw water storage tank level	
Steam generator pressure	
Turbine-driven pump rpm	
Motor-driven pumps amps	
Valve position indications	All motor-operated valves.
Direct valve position indication (# open)	Electro-Hydraulic LVs

generator low-low level in any two steam generators or loss of power to the Reactor Coolant Pump buses (sensed by bus undervoltage devices). PG&E has adequately described the system. Automatic initiation of the system is of prime importance because it eliminates human error events and thereby increases overall system reliability. A major concern is the fact that switch over to the RWSR or the FWST for backup cooling water is not automatic. In the event of loss of Net Positive Suction Head (NPSH) which causes a sudden demand for backup water, the pumps may fail before the establishment of flow or pump turnoff.

3.2 System Control Following Initiation

After initiation, flow control can be established through the level control valves on each Auxiliary Feedwater line to each steam generator. By observing the levels in the CST the operator can open the alternate water supply's motor-operated flow control valves at the appropriate time to prevent loss of NPSH.

3.3 Test and Maintenance Procedures and Unavailability

SNL was informed that the following applied to Test and Maintenance procedures:

3.3.1 Procedures

Diablo Canyon Maintenance Procedures E-87 for AFWS pump motors and M-27 and M-28 for AFWS pumps and turbine require completion of perfor-

mance tests (using surveillance test procedures). The tests verify pump operability following maintenance. The following Diablo Canyon surveillance test procedures affect the AFWS:

1. V-2B Auxiliary Feedwater and Containment Spray Valves - Exercises about half of the active AFWS valves during refueling outages.
2. V-2U Steam Generator Related Valves - Exercises the remaining active AFWS valves during refueling outages.
3. V-3P4 Exercising RWSR Supply to Auxiliary Feedwater Pumps, FCV-436, FCV-437. This test is performed when steam pressure exceeds 100 psig to verify proper operability of these motor-operated valves and their indicating lights. Improper completion of the test could leave the AFWS pumps' recirculation valves 32, 168, and 169 in the closed position; however monthly flow tests require that these valves be open.
4. P-5A(6A) Performance Test of Motor-Driven (Steam-Driven) Auxiliary Feed Pumps - These extensive tests verify proper pump performance over a wide range of operating conditions. It is performed following major maintenance and at 5-year intervals (Test P-6A is not yet written).

5. P-5B(6B) Routine Surveillance Test of Motor-Driven (Steam-Driven) Auxiliary Feedwater Pumps - These tests are run monthly to verify operability of the AFWS pumps. The remotely operated level control (flow control) valve is closed; the pump is test operated on recirculation; the LCVs (FCVs) are bumped open to verify flow to the steam generators; the pump is stopped; the LCVs are opened fully with their controllers left in manual (FCVs are opened fully). Procedure P-5B and its checklist are being revised to require operating and restoring the pump-running interlock override toggle switch in the control room and to specify that the controllers be returned to automatic. The three pumps are tested sequentially so the common human failure of leaving all LCVs and FCVs shut is possible.
6. P-6C Overspeed Trip of Steam-Driven Auxiliary Feed Pump - This test is conducted following refueling outages and verifies the turbine protection feature.

The test procedures are important in several respects. They verify the continued operability of standby equipment that must start on demand. They ensure no common cause problems are developing in an unmonitored fashion. They can uncover degradation or aging before complete failure

occurs. They are also the primary source of random failure-on-demand data. The tests also may have negative impacts because of improper restoration to normal service.

The following two Diablo Canyon Operating Procedures apply to the AFWS:

1. A-5 Steam Generators - Describes the use of the AFWS during startup (to about 5% power) and shutdown, and the transfer to and from main feed pumps. It also discusses hydrostatic testing and steam generator level recovery using the AFWS.
2. D-1 Auxiliary Feedwater System - Provides detailed (valve-by-valve) instructions for startup, operation, shutdown and clearance, and abnormal operation of the AFWS.

Neither procedure mentions the pump-running-interlock-override-toggle-switch on the AFWS panel in the control room and neither procedure tells the operator how to set up the electro-hydraulic LVCs for the standby (normal) condition. The procedures are in the process of revision.

PG&E sends copies of maintenance and operating procedures to NRC and to the NRC Resident Inspector for their review and comment.

3.3.2 Testing

Testing of the AFWS consists primarily of surveillance testing to satisfy the plant technical specifications and ASME Section XI requirements.

Monthly testing is performed on each AFW pump. For each pump test the level-control valves in the pump discharge lines are closed and the pump is started manually (from the Control Room or the Hot Shutdown Panel). Each pump is then run for at least 5 minutes to allow for stabilization of the system. Required pump data are then taken and recorded. After pump data have been taken, each level control valve in the pump discharge is sequentially cracked open to verify the associated flowpath operability. The AFW pump under test is then stopped and the level-control valves are opened fully. Successful completion of the monthly test requires that the AFW pump develop minimum differential pressure on recirculation flow, and the associated level control valves and flow path to the steam generator are operable. The pump tests are performed sequentially. During the test, if the AFWS is required to operate, the operator must restore the level-control valves to automatic.

Every 18 months the automatic starting circuits of the AFW pumps are tested. Satisfactory completion of this test requires that the AFW pump start upon receipt of a simulated automatic start signal.

All valves in the flow path that are not locked, sealed, or otherwise secured in position are verified to be in the correct position monthly. This test does not require valve cycling.

The condensate storage tank (CST) is checked to see that it is operable every 12 hours by verifying the volume of water it contains. When the fire water tank is the source of water to the AFWS, the volume of water contained in the firewater tank is verified every 12 hours.

3.3.3 Unavailability

The plant technical specifications limit the amount of time an auxiliary feedwater pump or auxiliary feedwater pump train may be out of service to 72 hours and limit the out-of-service time for the CST to 4 hours without the firewater tank and 7 days with the firewater tank.

3.3.4 Discussion of Failure Modes

Packing replacement and adjustment is the dominant cause of maintenance on valves. In most cases, this maintenance can be performed

with the valve in the correct position for system operation (fully open or fully closed). Valve repairs requiring disassembly of the valve, although not frequently, may have a major impact on system availability because of system isolation requirements necessary to safely perform this maintenance. Those valves which require full AFWS shutdown for repair also require a plant shutdown (per technical specifications) and, therefore, do not contribute to the maintenance unavailability of the AFWS. Those valves requiring maintenance which only need a single AFW pump train to be shut down do contribute to maintenance unavailability of the AFWS. Valves which are periodically cycled, which have a throttling action, or which are in a high-energy system are the dominant contributors to this unavailability. The steam supply valve to the turbine-driven AFW pump, PCV-95, is the only valve in the system which is periodically cycled, performs a throttling action, and is in a high-energy system. PCV-95 maintenance is included in the maintenance unavailability of the turbine driven pump train.

Pump maintenance consists of a range of actions from major disassembly to packing adjustment. For the AFW pumps, most maintenance performed requires isolation of the pump from the system, and, therefore, contributes to the maintenance unavailability of the pump train.

The maintenance on large motors ranges from inspection and cleaning to major disassembly. The prevalent failure mode is bearing failure which requires partial disassembly of the motor. All maintenance of

the AFW pump motors contributes to maintenance unavailability and is included in the pump train maintenance contribution.

Turbine maintenance can range from simple adjustments to major disassembly. A review of Licensee Event Reports from January 1972 to April 1978 revealed only one reported failure of a turbine in an AFWS. This failure was due to a casing steam leak discovered during startup after routine maintenance had been performed. Turbine failure is included in the maintenance contribution to unavailability of the turbine-driven pump train.

Motor-operated valve (MOV) control circuit failures occur with moderate frequency. Repair generally consists of troubleshooting and defective component replacement or adjustment. Only one valve in the AFWS receives an automatic open signal upon system demand, FCV-95. All other MOVs are in the correct position for system operation and failure of the control circuit does not affect system operation. During repair of a MOV control circuit, manual operation of the valve is always available. For these reasons, control-circuit failures for MOVs are not included in the maintenance unavailability contribution.

AFW pump motor breakers and control circuits require periodic maintenance and repair. Because the 4160 V breakers are interchangeable between 4160 V cubicles, and spare breakers are available, major breaker repair is not included in the maintenance unavailability of the motor-

driven pump trains. All other control and breaker maintenance is included in the unavailability of the motor-driven AFW pump trains.

3.4 Adequacy of Emergency Procedures

SNL was informed that the following applied to Emergency Procedures:

Every emergency operating procedure (EOP) that applies to transients leading to reactor trip calls upon (or should call upon) the AFWS.

The existing Diablo Canyon EOPs are inconsistent in their discussions of the AFWS. Some ignore it; some say to check that the pumps have started; some say only to throttle AFWS flow; etc. None warn the operator that all pumps could be lost quickly (in less than about 5 minutes) on loss of suction. None explain how to shift suction supply. Improvements could increase the likelihood of effective operator response to recoverable failures. The existing EOPs are discussed below.

1. OP-1 Loss of Coolant Accident - Does not mention the AFWS or refer to other EOPs. For small breaks, initiation of steam dump to assist cooldown is specified. Neither AFWS nor primary bleed and feed are discussed.
2. OP-2A Steam Line break - Directs the operator to isolate AFW to a faulty steam generator in a subsequent action, but does not mention startup or verification of AFWS flow.
3. OP-2B Feedwater Line break - Lists actuation of AFWS as an automatic action. An immediate operation action is to

verify that the pumps have started and a subsequent operator action is to isolate a faulty steam generator.

4. OP-4 Loss of Electric Power - Lists two AFWS automatic actions. First, turbine pump start, and second, motor pump start following the diesel generator loading sequence. The immediate operator actions for AFWS are to check that all pumps started, that valves opened, and that there is flow to the steam generators. The subsequent actions include shutdown of the turbine pump at >20% level and continued motor pump operation in AUTO.
5. OP-5 Reactor Trip without Safety Injection - Immediate operator actions include checking for an adequate heat sink by verifying steam dump valves open and, if main feedwater is lost, checking that the AFWS pumps started. The subsequent actions bring the AFWS on line if not already running and verify correct operation by status lights, AFWS pressures and flows, and LCVs in AUTO above 33% level.
6. OP-7 Loss of Condenser Vacuum - Lists the start of both motor-driven AFWS pumps as automatic actions. Immediate operator actions include verifying that all automatic actions have occurred. A subsequent action is to control AFWS flow to each steam generator to prevent excessive cooldown and/or water hammer.
7. OP-8 Control Room Inaccessability - AFWS pumps are checked running and are used to control steam generator levels

at 33% as subsequent actions after the operator has moved to the hot shutdown panel.

8. OP-9 Loss of a Reactor Coolant Pump - The immediate and subsequent operator actions fall into two cases, with and without reactor trip. Only the reactor trip case is of interest. The first immediate action is to follow the trip procedure, but this action is followed by a series of additional immediate and subsequent actions much less detailed than in the reactor trip procedure. The only reference to the AFWS is a subsequent action to regulate steam generator levels by use of the auxiliary feedwater pumps.
9. OP-15 Loss of Feedwater Flow - Lists the start of the motor-driven AFWS pumps as an automatic action along with the possible start of the turbine pump. The immediate operator actions include checking that the reactor has tripped (the reactor trip procedure is not mentioned), checking that the motor driven pumps have started, checking that the valves are open and there is flow into the steam generators. Also, under Anticipated Transient Without Scram (ATWS), the turbine pump is started, valves are checked to see that they are open, and flow into the steam generators is verified. The subsequent actions call for maintenance of steam generator levels using AFWS pumps and checking that the turbine pump

started should low-low level occur in any two steam generators.

The emergency procedures are undergoing revision. Most have been altered and most correct the concerns cited above. A new Emergency Operating Procedure, OP-0 Reactor Trip with Safety Injection, has been written. This procedure is a general diagnostic which directs the operator to other procedures for subsequent actions. It mentions a check on the AFW pump flows and other general procedures that are to be added. It consolidates the others into a more cohesive package and avoids many of the previous inconsistencies.

As with Maintenance and Operating Procedures, Emergency Operating Procedures are sent to NRC and to the NRC resident inspector for their review and comment.

Emergency Procedures are very necessary as a backup to automatic operations and for surveillance and control of the AFWS operation after system initiation. This affects system reliability by allowing, in the case of an automatic starting system like Diablo Canyon, a human action backup if sufficient time is available. This backup increases AFWS reliability; however, extreme care on the part of the operators coupled with a detailed knowledge of system interactions is required to keep from defeating necessary functioning safety systems.

3.5 Adequacy of Power Sources and Separation of Power Sources

At Diablo Canyon the motor-driven AFWS pumps are supplied from different buses which are, if there is a loss of offsite power, powered from separate diesel generators. Separation of power systems is necessary to eliminate common-cause failure events from reliability consideration. In doing so AFWS reliability is increased.

3.6 Availability of Alternate Water Sources

The primary alternate source of feedwater is the Raw Water Storage Reservoir except in the case of a seismic event, in which case the alternate source is the Fire Water Storage Tank. The reliability report allows an operator 30 minutes to switch to the alternate source when the CST valve is closed or plugged and the AFW pumps are tripped. The report allows 5 minutes for operator action to trip the AFWPs if the CST valve is closed or plugged. Diablo Canyon has no automatic pump trip on low NPSH signal and no automatic system to valve in the alternate feedwater. The time allowances for the two human action events are questionable. Automation of the two events as recommended by NUREG-0611 would increase AFWS reliability.

3.7 Potential Common-Mode Failures

PG&E made an extensive common-mode failure study and identified nine third-order cutsets with common susceptibilities in common locations.

They were electrical train cutsets that are well protected from the following identified susceptibilities:

1. Conducting Medium - None present. Even if brought into the area, the equipment is protected.
2. Impact - No sources present; well protected from portable sources.
3. Temperature - Fire is a possibility, but would need to be wide-spread and severe to cause damage. Such fires have very low probability of occurrence and fire protection equipment must fail.
4. Corrosion - No source of sufficient moisture; regular maintenance.
5. Grit - Portable sources could be a problem but equipment is well protected and heavy dirt is not generated during power operations.
6. Vibration - No significant sources.
7. Explosion - Very unlikely; only portable sources and they are carefully controlled. Sufficient separation exists to offer some protection.

The PG&E systems interaction program is systematically lowering the likelihood of even single component failures due to environmental factors. The most significant impediment to common environmental causes at Diablo Canyon is the separation factor. Only the nine third-order cutsets discussed above have all basic events in the same location. The effect of these on the AFWS reliability is negligible.

3.8 Application of Data Presented in NUREG-0611

The Pickard, Lowe and Garrick report contained a table which included all basic fault tree events. Most of the assessments for these events were taken from NUREG-0611. In the final analysis some of the first order events were adjusted by the use of recovery factors. Although recovery factors have their place, it was felt that the time allowed for recovery was too long and should not have been used. NUREG-0611 does not mention recovery factors and does not give data for any recovery events. In this analysis it is used to soften the effect of a first-order failure event and thereby biases the comparison of Diablo Canyon to operating nuclear power stations.

3.9 Search for Single Failure Points

The only single failure point (SFP), a first-order mechanical failure event, found for Cases 1 and 2 was the failure of CST outlet valve number 1-671. This was later changed to a second-order cutset as described in paragraph 3.8 above. Numerous SFPs were identified for Case 3 since, by design, it is a single-channel system.

3.10 Human Factors/Errors

Human factors/errors were considered by PG&E and combined into the cutsets listed for the basic mechanical failure fault tree. The unavailability numbers generated by this process were summed and reported for each case. Automation is a major factor in decreasing the effect of human error on reliability. At Diablo Canyon there is

no automatic cutoff of the AFWS pumps on a low NPSH signal nor is there an automatic opening of the valves which isolate the alternate supply of feedwater.

3.11 NUREG-0611 Recommendations, Long and Short-Term

3.11.1 Short-Term Generic Recommendations

I. Technical Specification Time Limit on AFWS Train Outage.

Recommendation GS-1

The licensee should propose modifications to the Specifications to limit the time that one AFW system pump and its associated flow train and essential instrumentation can be inoperable. The outage time limit and subsequent action time should be as required in current Standard Technical Specifications, i.e., 72 and 12 hours, respectively.

Response

The Diablo Canyon AFWS design consists of two trains powered by vital busses and one train powered by the steam supply system. Draft Diablo Canyon Technical Specification 3.7.1.2. requires that all three trains of Auxiliary Feedwater be operable, including instrumentation, during power operation, start-up, and hot standby modes. The time limit for one train of AFWS inoperable is 72 hours. Subsequent actions required in the event of continued inoperability of one train is: be in at

least hot standby within the next 6 hours and be in at least hot shutdown within the following six (6) hours.

II. Technical Specification Administrative Controls on Manual Valves--Lock and Verify Position

Recommendation GS-2

The licensee should lock open single valves or multiple valves in series in the AFWS pump suction piping, and lock open other single valves or multiple valves in series that could interrupt all AFWS flow. Monthly inspections should be performed to verify that these valves are locked and in the open position. These inspections should be proposed for incorporation into the surveillance requirements of the plant Technical Specifications. See Recommendation GL-2 for the long term resolution of this concern.

Response

There is one normally open, manual valve in the common suction piping of the Diablo Canyon AFW pump. This valve will be locked, sealed, or otherwise secured in the open position whenever the plant is in a power operation, start-up, or hot shutdown mode. A proposed Technical Specification revision will require that correct valve alignment is verified monthly.

III. AFWS Flow Throttling - Water Hammer

Recommendation GS-3

The licensee has stated that it throttles AFWS flow to avoid water hammer. The licensee should reexamine the practice of throttling AFWS flow to avoid water hammer.

The licensee should verify that the AFWS will supply on demand sufficient initial flow to the necessary steam generators to assure adequate decay heat removal following loss of main feedwater flow and a reactor trip from 100% power. In cases where this reevaluation results in an increase in initial AFWS flow, the licensee should provide sufficient information to demonstrate that the required initial AFWS flow will not result in plant damage due to water hammer.

Response

The Diablo Canyon steam generators were modified in January 1976 to preclude the occurrence of feedwater line water-hammer events. The modifications consisted of retrofitting the feedwater spargers with "J-tubes." Tests at operating plants have demonstrated that the "J-tubes" modification does, in fact, preclude water-hammer events.

The Diablo Canyon AFWS control valves will be full open at the start of any event requiring the automatic initiation of the AFWS. Plant operating procedures require that the valves remain unthrottled until the steam generator water levels are recovered, at which time the control valves will be throttled, as required either automatically or manually to maintain the steam generator water levels. The AFWS control valves are also automatically throttled to limit flow to a depressurized steam generator. This feature protects against destructive runout of the motor-driven AFWS pumps.

IV Emergency Procedures for Initiating Backup Water Supplies

Recommendation GS-4

Emergency Procedures for transferring to alternate sources of AFW supply should be available to the plant operators. These procedures should include criteria to inform the operators when, and in what order, the transfer to alternate water sources should take place. The following cases should be covered by the procedures:

- (1) The case in which the primary water supply is not initially available. The procedures for this case should include any operator actions required to protect the AFW system pumps against self-damage before water flow is initiated.

- (2) The case in which the primary water supply is being depleted. The procedure for this case should provide for transfer to the alternate water sources before the primary water supply is drained.

Response

Emergency procedures are being revised. The revised procedures will incorporate the guidelines of the Westinghouse Owners Group Task Force on Emergency Procedures. The revised procedures will include the operator actions required to align secondary water sources for the case where the primary water source is initially not available and the case where the primary water source is being depleted. The revised procedures will be made available for NRC review.

- V Emergency Procedures for Initiating AFW Flow Following a Complete Loss of Alternating Current Power

Recommendation GS-5

The as-built plant should be capable of providing the required AFW flow for at least 2 hours from one AFW pump train, independent of any ac power source. If manual AFW system initiation of flow control is required following a complete loss of ac power, emergency procedures should be established for manually initiating and controlling the system under these conditions. Since

the water for cooling of the lubricating oil for the turbine-driven pump bearings may be dependent on ac power, design or procedural changes shall be made to eliminate this dependency as soon as practicable. Until this is done, the emergency procedures should provide for an individual to be stationed at the turbine-driven pump in the event of the loss of all ac power to monitor pump bearing and/or lubricating oil temperatures. If necessary, this operator would operate the turbine-driven pump in an on-off mode until ac power is restored. Adequate lighting powered by dc power sources and communications at local stations should also be provided if manual initiation and control of the AFW system is needed. (See Recommendation GL-3 for the longer-term resolution of this concern).

Response

The Diablo Canyon AFWS will be modified at or prior to the first refueling so that one train of AFW is capable of delivering the required flow, independent of off-site and on-site ac power. This train will consist of a steam-driven AFW Pump that delivers flow to all four steam generators, a steam supply stop valve powered from a vital dc bus (station batteries), automatic AFWS actuation instrumentation powered from a vital instrument ac bus, and steam generator level

and AFW flow indication instrumentation powered from a vital instrument ac bus. In the event of loss of on-site ac power, the vital instrument ac busses are powered from the station batteries through an inverter. The steam-turbine-driven AFW pump has no dependence on ac power. Bearing lubricating oil cooling water is taken from the pump discharge. Appropriate AFWS operating procedures will be prepared for loss of off-site and on-site ac power.

VI AFWS Flow Path Verification

Recommendation GS-6

The licensee should confirm flow path availability of an AFW system flow train that has been out of service to perform periodic testing or maintenance as follows:

- (1) Procedures should be implemented to require an operator to determine that the AFW system valves are properly aligned and a second operator to independently verify that the valves are properly aligned.
- (2) The licensee should propose Technical Specifications to assure that, before plant start-up following an extended cold shutdown, a flow test would be performed to verify the normal flow path from the primary AFW system water source to the steam generators. The

flow test should be conducted with AFW system valves in the normal alignment.

Response

The Diablo Canyon AFWS periodic testing and maintenance procedures include requirements to return the system valves to their proper alignment after the testing or maintenance activity. Presently they do not include requirements for an independent verification by a second operator.

The Diablo Canyon design requires the AFWS to function during plant start-up from cold shutdown conditions. Flow path availability from the primary water source to the steam generators is thus demonstrated during the normal course of plant start-up.

VII Non-Safety Grade, Nonredundant AFWS Automatic Initiation Signals

Recommendation GS-7

The licensee should verify that the automatic start AFW system signals and associated circuitry are safety-grade. If this cannot be verified, the AFW system automatic initiation system should be modified

in the short-term to meet the functional requirements listed below. For the longer term, the automatic initiation signals and circuits should be upgraded to meet safety-grade requirements as indicated in Recommendation GL-5.

- (1) The design should provide for the automatic initiation of the auxiliary feedwater system flow.
- (2) The automatic initiation signals and circuits should be designed so that a single failure will not result in the loss of auxiliary feedwater system function.
- (3) Testability of the initiation signals and circuits shall be a feature of the design.
- (4) The initiation signals and circuits should be powered from the emergency buses.
- (5) Manual capability to initiate the auxiliary feedwater system from the control room should be retained and should be implemented so that a single failure in the manual circuits will not result in the loss of system function.
- (6) The ac motor-driven pumps and valves in the auxiliary feedwater system should be included in the automatic actuation (simultaneously and/or sequential) of the loads to the emergency buses.

- (7) The automatic initiation signals and circuits shall be designed so that their failure will not result in the loss of manual capability to initiate the AFW system from the control room.

Response

The Diablo Canyon Auxiliary Feedwater System presently meets all of the listed functional requirements. The required automatic AFW actuation signals and associated circuitry are safety-grade.

VIII Automatic Initiation of AFWS

Recommendation GS-8

The licensee should install a system to automatically initiate AFW system flow. This system need not be safety-grade; however, in the short-term, it should meet the criteria listed below, which are similar to Item 2.k.7a of NUREG-0578. For the longer term, the automatic initiation signals and circuits should be upgraded to meet safety-grade requirements as indicated in Recommendation GL-2.

- (1) The design should provide for the automatic initiation of the auxiliary feedwater system flow.

- (2) The automatic initiation signals and circuits should be designed so that a single failure will not result in the loss of auxiliary feedwater system function.
- (3) Testability of the initiating signals and circuits should be a feature of the design.
- (4) The initiating signals and circuits should be powered from the emergency buses.
- (5) Manual capability to initiate the auxiliary feedwater system from the control room should be retained and should be implemented so that a single failure in the manual circuits will not result in the loss of system function.
- (6) The ac motor-driven pumps and valves in the auxiliary feedwater system should be included in the automatic actuation (simultaneous and/or sequential) of the loads to the emergency buses.
- (7) The automatic initiation signals and circuits should be designed so that their failure will not result in the loss of manual capability to initiate the AFW system from the control room.

Response

The Diablo Canyon Auxiliary Feedwater System presently meets all of the listed functional requirements. The required automatic AFW actuation signals and associated circuitry are safety-grade.

3.11.2 Additional Short-Term Recommendations

I. Primary AFW Water Source Low-Level Alarm

Recommendation

The licensee should provide redundant level indication and low-level alarms in the control room for the AFW system primary water supply to allow the operator to anticipate the need to make up water or transfer to an alternate water supply and prevent a low pump suction pressure condition from occurring. The low-level alarm setpoint should allow at least 20 minutes for operator action, assuming that the largest capacity AFW pump is operating.

Response

The primary water source for the Diablo Canyon Auxiliary Feed-water System is the Condensate Storage Tank (CST). CST level indication is available locally at the tank, at the remote hot shutdown panel, and in the control room. The level indication instrument channels presently are neither redundant nor safety-grade. They are, however, seismically qualified. They will be upgraded to be redundant and safety-grade.

A CST Low-Low Level Alarm is annunciated in the control room. The alarm setpoint would presently give the plant operator 16

minutes notice of the need to transfer the AFWS to a secondary water source. The Low-Low Level Alarm setpoint will be changed to give the operator 20 minutes of AFW pump running time before the secondary water source must be cut in. The Low-Low-Level Alarm instrument circuit is safety-grade.

II AFW Pump Endurance Test

Recommendation

The licensee should perform a 72-hour endurance test on all AFW system pumps, if such a test or continuous period of operation has not been done already. Following the 72-hour pump run, the pumps should be shut down and cooled down and then restarted and run for 1 hour. Test acceptance criteria should include demonstrating that the pumps remain within design limits with respect to bearing/bearing oil temperatures and vibration and that pump room ambient conditions (temperature, humidity) do not exceed environmental qualification limits for safety-related equipment in the room.

Response

An endurance test of the Diablo Canyon AFWS will be performed before start-up. The endurance test procedures and acceptance criteria will be made available to the NRC for comment before the test.

III Indication of AFW Flow to the Steam Generator

Recommendation

The licensee should implement the following requirements as specified by Item 2.1.7.b on Page A-32 of NUREG-0578:

- (1) Safety-grade indication of AFW flow to each steam generator should be provided in the control room.
- (2) The AFW flow instrument channels should be powered from the emergency buses consistent with satisfying the emergency power diversity requirements for the AFW system set forth in the Auxiliary Systems Branch Technical Position 10-1 of the Standard Review Plan, Section 10.4.9.

Response

The Diablo Canyon AFWS design includes indication of AFW flow to each steam generator in the control room and at the remote

hot shutdown panel. The instrument channels are safety-grade and powered from separate emergency vital buses.

IV AFWS Availability During Periodic Surveillance Testing

Recommendation

Licensees with plants which require local manual realignment of valves to conduct periodic test on one AFW system train, and which have only one remaining AFW train available for operation, should propose Technical Specifications to provide that a dedicated individual who is in communication with the control room be stationed at the manual valves. Upon instruction from the control room, this operator would realign the valves in the AFW system from the test mode to its operational alignment.

Response

The Diablo Canyon AFWS design includes three trains. This recommendation, therefore, is not applicable. It should be noted, however, that periodic test of the Diablo Canyon AFWS will not require local manual realignment of valves. The required valve realignment is accomplished from the control room. System realignment from the test mode to the normal AFWS operational mode is available from the control room.

3.11.3 Long-Term Generic Recommendations

I. Automatic Initiation of AFWs

Recommendation GL-1

For plants with a manual-starting AFW system, the licensee should install a system to automatically initiate the AFW system flow. This system and associated automatic initiation signals should be designed and installed to meet safety-grade requirements. Manual AFW system start and control capability should be retained with manual start serving as backup to automatic AFW system initiation.

Response

See comparison to Recommendation GS-8.

II Single Valves in the AFWS Flow Path

Recommendation GL-2

Licensees with plant designs in which all (primary and alternate) water supplies to the AFW systems pass through valves in a single flow path, should install redundant parallel flow paths (piping and valves).

Licensees with plant designs in which the primary AFW system water supply passes through valves in a single flow path, but

alternate AFW system water supplies connect to the AFW system pump suction piping downstream of the above valve(s), should install redundant valves parallel to the above valve(s) or provide automatic opening of the valve(s) from the alternate water supply upon low pump suction pressure.

The licensee should propose Technical Specifications to incorporate appropriate periodic inspections to verify the valve positions into the surveillance requirements.

Response

The common supply from the primary water source to the AFWS pumps contains one normally open valve. The alternate water source for the AFW pumps connects downstream of this valve. See response to Recommendation GS-2 for additional information.

III Elimination of AFWS Dependency on Alternating Current Power Following a Complete Loss of Alternating Current Power

Recommendation GL-3

At least one AFW system pump and its associated flow path and essential instrumentation should automatically initiate AFW system flow and be capable of being operated independently of

any ac power source for at least 2 hours. Conversion of dc power to ac is acceptable.

Response

See response to Recommendation GS-5.

IV Prevention of Multiple Pump Damage Due to Loss of Suction
Resulting from Natural Phenomena

Recommendation GL-4

Licensees having plants with unprotected normal AFW system water supplies should evaluate the design of their AFW systems to determine if automatic protection of the pumps is necessary following a seismic event or a tornado. The time available before pump damage, the alarms and indications available to the control room operator, and the time necessary for assessing the problem and taking action should be considered in determining whether operator action can be relied on to prevent pump damage. Consideration should be given to providing pump protection by means such as automatic switchover of the pump suctions to the alternate safety-grade source of water, automatic pump trips on low suction pressure, or upgrading the normal source of water to meet seismic Category I and tornado protection requirements.

Response

The primary water source for the AFWS is Seismic Category I. The primary water source has been evaluated for the potential for damage due to tornado.

V Non-Safety Grade, Nonredundant AFWS Automatic Initiation Signals

Recommendation GL-5

The licensee should upgrade the AFW system automatic initiation signals and circuits to meet safety-grade requirements.

Response

See response to Recommendation GS-7.

4. Major Contributors to Unreliability

PG&E lists the top events together with their rank order and unavailability for each of the three cases. These are shown in Tables 2, 3, and 4. The sum includes all events or cutsets considered. The sum is plotted on Figure 2 to show how Diablo Canyon compares with operating units as reported by NUREG-0611.

SNL does not agree with the assessment of the Rank 1 event on Tables 2 and 3 because a 5-minute time for operator action before pump

TABLE 2

DOMINANT CONTRIBUTORS TO CONDITIONAL UNAVAILABILITY

CASE 1. LOSS OF MAIN FEEDWATER

Rank	Event Description	Unavailability
1	Human Error: CST outlet valve 1-671 closed and no operator action to trip the AFWPs (5 minutes).	2.82×10^{-5}
2	Human Error: CST outlet valve 1-671 closed and AFWPs tripped and no operator action to restore a water supply (30 minutes).	4.40×10^{-6}
3	Test and Maintenance: Turbine driven AFWP down for maintenance and random system failures.	1.08×10^{-6}
4	Test and Maintenance: Motor driven AFWP 1-3 down for maintenance and random system failures.	9.19×10^{-7}
5	Test and Maintenance: Motor driven AFWP 1-2 down for maintenance and random system failures.	9.19×10^{-7}
6	Common Cause--Human Error: All LCVs in incorrect position after test and no operator action to open LCVs (30 minutes).	6.50×10^{-7}
7	Human Error: Turbine controls failure or FCV-95 controls failure and no operator action to start turbine driven pump (30 minutes).	1.31×10^{-7}
8	Nonrecoverable Random Failure: Motors for AFWP 01-2 and 01-3 fail and FCV-95 does not open (mechanical failure).	1.76×10^{-8}
Sum for all 786 Events or Cutsets		3.7×10^{-5}

TABLE 3
DOMINANT CONTRIBUTORS TO CONDITIONAL UNAVAILABILITY
CASE 2 - LOSS OF MAIN FEEDWATER AND LOSS OF OFFSITE POWER

Rank	Event Description	Unavailability
1	Human Error: CST outlet valve 1-671 closed and no operator action to trip the AFWPs (5 minutes).	2.82×10^{-5}
2	Test and Maintenance: Turbine driven AFWP down for maintenance and random system failures.	1.53×10^{-5}
3	Human Error: CST outlet valve 1-671 closed and AFWPs tripped and no operator action to restore a water supply (30 minutes).	4.4×10^{-6}
4	Test and Maintenance: Motor driven AFWP 1-3 down for maintenance and random system failures.	3.00×10^{-6}
5	Test and Maintenance: Motor driven AFWP 1-2 down for maintenance and random system failures.	3.00×10^{-6}
6	Nonrecoverable Random Failure: Failure of electric buses F and H and FCV-95 does not open (mechanical failure).	1.50×10^{-6}
7	Nonrecoverable Random Failure: Failure of electric buses F and H and PV-39 fails closed.	1.50×10^{-6}
8	Nonrecoverable Random Failure: Failure of electric buses F and H and turbine-driven pump fails mechanically.	1.37×10^{-6}
9	Common Cause--human Error: All LCVs in incorrect position after test and no operator action to open LCVs (30 minutes).	6.50×10^{-7}
10	Human Error: Turbine controls failure or FCV-95 controls failure and no operator action to restart turbine-driven pump (30 minutes).	3.18×10^{-7}
Sum for all 786 Events or Cutsets		6.1×10^{-5}

TABLE 4

DOMINANT CONTRIBUTORS TO CONDITIONAL UNAVAILABILITY
CASE 3 - LOSS OF MAIN FEEDWATER AND LOSS OF ALL AC POWER

Rank	Event Description	Unavailability
1	Test and Maintenance: Turbine pump train down for maintenance.	8.02×10^{-3}
2	Nonrecoverable Random Failure: FCV-95 does not open (mechanical failure).	1.10×10^{-3}
3	Nonrecoverable Random Failure: PV-39 does not open (mechanical failure).	1.10×10^{-3}
4	Nonrecoverable Random Failure: Turbine pump fails (mechanical failure).	1.0×10^{-3}
5	Human Error: Turbine controls failure or FCV-95 controls failure and no operator action to restart pump (30 minutes).	2.64×10^{-4}
6	Nonrecoverable Random Failure: Turbine train valve, check valve 135.	1.00×10^{-4}
7	Nonrecoverable Random Failure: Turbine train valve, gate valve 135.	1.00×10^{-4}
8	Nonrecoverable Random Failure: Turbine train butterfly valve 124.	1.00×10^{-4}
9	Nonrecoverable Random Failure: Turbine train butterfly valve 121.	1.00×10^{-4}
10	Nonrecoverable Random Failure: Turbine train valve, check valve 121.	1.00×10^{-4}
11	Human Error: CST outlet valve 1-671 closed and no operator action to trip to AFWPs (5 minutes).	2.82×10^{-5}
12	Human Error: CST outlet valve 1-671 closed and AFWP tripped and no operator action to restore a water supply (30 minutes).	4.40×10^{-6}
13	Common Cause--Human Error: All LCVs in incorrect position after test and no operator to open LCVs (30 minutes).	6.50×10^{-7}
	Sum for all 17 Events or Cutsets	1.2×10^{-2}

failure in the event of no NPSH has not been established. The operator action should not be considered and the unavailability increased to 1×10^{-4} , the value assigned to the CST outlet valve 1-671 being closed. This value is combined with the unavailability of the other cutsets of lesser rank and plotted on Figure 2. All other values seem appropriate.

5. Conclusions

The following conclusions resulted from this review:

1. Compliance to Letter of March 10, 1980

PG&E has complied with requirement (b) of the letter which states:

"(b) perform a reliability evaluation similar in method to that described in Enclosure 1 that was performed for operating plants and submit it for staff review." Enclosure 1 to the letter of March 10th provides the applicable portions of NUREG 0611 which deal with the Auxiliary Feedwater Systems.

2. Major Contributions to Unreliability

The PG&E report adequately discussed the major contributors to unreliability for the three cases (1) LMFW, Loss of Main Feedwater, (2) LMFW/LOOP, Loss of Main Feedwater/Loss of offsite power, and (3) LMFW/LAC, Loss of Main Feedwater/Loss of all ac power. The major contributor in Case 1 and 2 is the failure or incorrect positioning of the Condensate Storage Tank (CST) outlet valve 1-671 combined with no operator action to trip the Auxiliary Feedwater (AFW) pumps. The valve, 1-671, is in the common pipe which provides water from the CST to all AFW pumps. The major

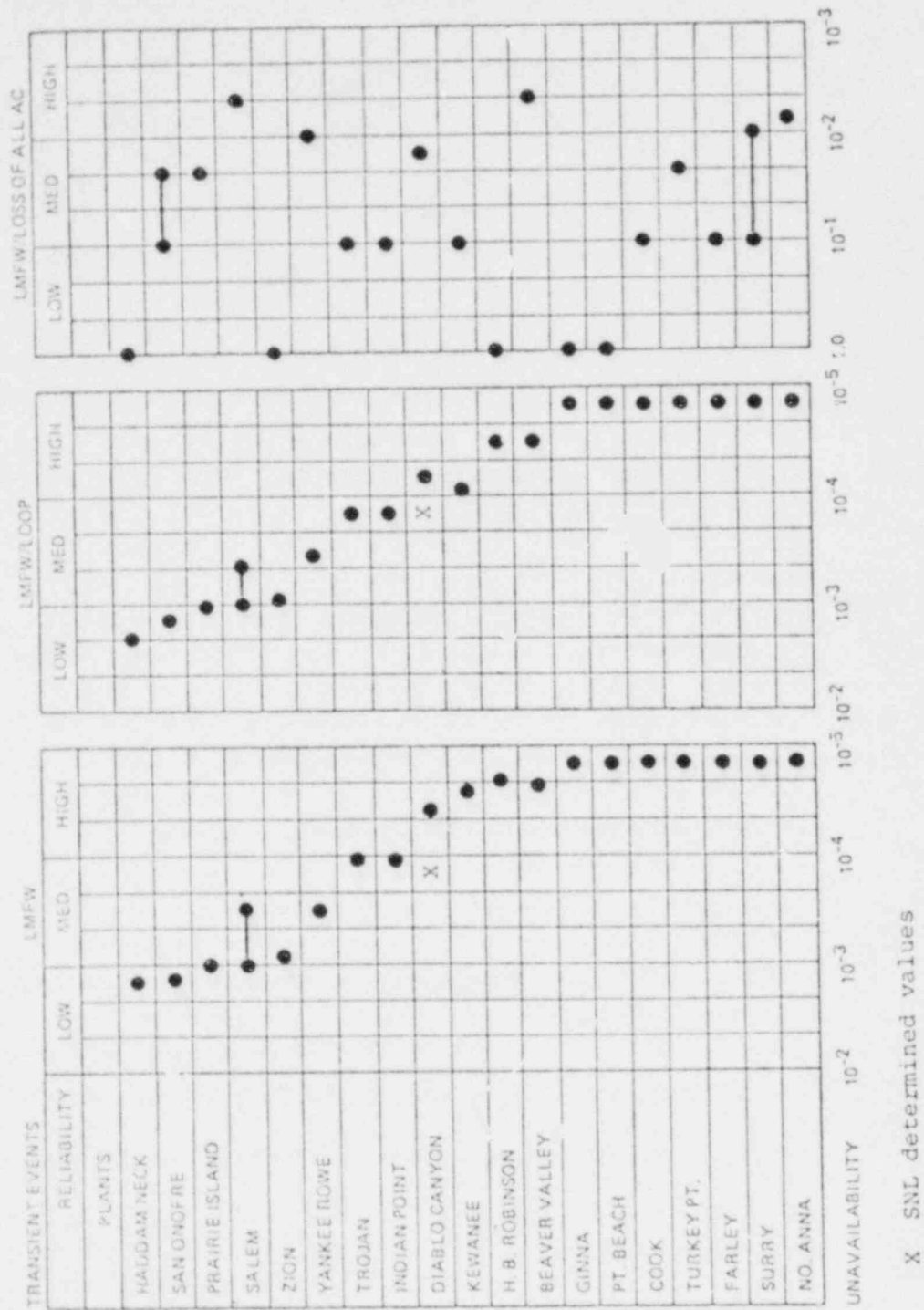


FIGURE 2. RELIABILITY CHARACTERIZATIONS FOR APWS DESIGNS IN PLANTS USING THE WESTINGHOUSE NSSS

contributors in Case 3 were the steam turbine and its supporting systems.

3. Method Used by PG&E

The method used by PG&E was in general agreement with the method used in NUREG-0611. All areas of the study were adequately addressed.

4. Final Assessment by PG&E

The final assessment made by PG&E places Diablo Canyon at the high end of the range of reliability reported in NUREG-0611 for operating Westinghouse plants. Sandia is not in agreement with this assessment for Case 1 and 2 because of questionable recovery factors used to lower the failure assessment of critical basic events. Sandia concludes that for Case 1 and 2 the reliability should be in the medium range.

References

1. 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.
2. PLG-0140, Subject: Reliability Analysis of Diablo Canyon Auxiliary Feedwater System by Dennis C. Bley, David M. Wheeler, Carroll L. Cate, Daniel W. Stillwell and B. John Jarrick, Preliminary issue dated July 8, 1980.
3. NUREG-0611 "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Westinghouse-Designed Operating Plants" dated January 1980.*
4. Memo Phillip A. Crane Jr. PG&E to John F. Stolz NRC Re. Docket No. 50-275, Docket No. 50-323, Diablo Canyon Units 1 and 2 dated April 8, 1980.
5. 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" date August 6, 1980.
6. PLG-0140 Subject: Reliability Analysis of Diablo Canyon Auxiliary Feedwater System by Dennis C. Bley, David M. Wheeler, Carroll L. Cate, David W. Stillwell and B. John Garrick. Revision 3 dated September 1980.
7. Tauche W., "Loss of Feedwater Induced Loss of Coolant Accident Analysis Report, "WCAP-9744, May 1980.

*Available for purchase from the NRC/GPO Sales Program, U.S. Nuclear Regulatory Commission, Washington, DC 20555, and/or the National Technical Information Service, Springfield, VA 22161.

Distribution:

U. S. Nuclear Regulatory Commission (130 copies for AN)
Distribution Contractor
7300 Pearl Street
Bethesda, MD 20014

Armand Lakner
U. S. Nuclear Regulatory Commission
Washington, DC 20555

1222	G. H. Bradley
3141	L. J. Erickson (5)
3151	W. L. Garner (3) (for DOE/TIC)
3154-3	C. H. Palin (25) (for NRC distribution to NTIS)
4400	A. W. Snyder
4414	J. W. Hickman
8214	M. A. Pound

NRC FORM 335 U.S. NUCLEAR REGULATORY COMMISSION BIBLIOGRAPHIC DATA SHEET		1. REPORT NUMBER (Assign only DDC) NUREG/CR-1925 SAND81-0242	
4. TITLE AND SUBTITLE (Add Volume No., if appropriate) Diablo Canyon Nuclear Power Station Unit 1 Auxiliary Feedwater System Reliability Study Evaluation		2. (Leave blank)	
7. AUTHOR(S) George H. Bradley, Jr.		3. RECIPIENT'S ACCESSION NO. 	
9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code) Sandia National Laboratories Albuquerque, NM 87185		5. DATE REPORT COMPLETED MONTH: February YEAR: 1981 DATE REPORT ISSUED MONTH: July YEAR: 1981	
12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code) Office of Nuclear Reactor Regulation Division of Safety Technology U.S. Nuclear Regulatory Commission Washington, DC 20555		6. (Leave blank) 8. (Leave blank)	
13. TYPE OF REPORT Reliability Study Evaluation		10. PROJECT/TASK/WORK UNIT NO. 11. CONTRACT NO. FIN A1121	
15. SUPPLEMENTARY NOTES		PERIOD COVERED (Indicate dates) July 1980 - December 1980	
16. ABSTRACT (200 words or less) One of the important safety systems involved in the mitigation of the Three Mile Island accident was determined to be the Auxiliary Feedwater System (AFWS); each operating plant's AFWS was studied and analyzed. The results for Westinghouse designed plants were reported in NUREG-0611. Prior to obtaining an operating license, the applicant for each non-operating plant is required to perform a reliability analysis of his AFWS in a manner similar to the study made in NUREG-0611. <u>Conclusions</u> 1. Pacific Gas and Electric Company (PG&E) has complied with requirement (b) of an NRC letter which states: "(b) perform a reliability reevaluation similar in method to that described in Enclosure 1 that was performed for operating plants and submit it for staff review." Enclosure 1 to the letter provides the applicable portions of NUREG-0611 which deal with the Auxiliary Feedwater Systems. 2. The PG&E report adequately discussed the major contributors to unreliability for the three cases: (1) LMFw, Loss of Main Feedwater, (2) LMFw/LOOP, Loss of Main Feedwater/Loss of Offsite Power, and (3) LMFw/LAC, Loss of Main Feedwater/Loss of All AC Power.		14. (Leave blank)	
17. KEY WORDS AND DOCUMENT ANALYSIS Reliability Auxiliary Feedwater System (AFWS) Valve Pump		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 \$

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

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, \$300

POSTAGE AND FEES PAID
U.S. NUCLEAR REGULATORY
COMMISSION



NUREG/CR-1925

DI-
CANYON NUCLEAR POWER STATION
RELIABILITY STUDY EVALUATION

120555064215 2 AN
US NRC
ADM DOCUMENT CONTROL DESK
PCR
016
WASHINGTON DC 20555