UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

BEFORE THE ATOMIC SAFETY AND LICENSING APPEAL BOARD

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| PACIFIC GAS AND ELECTRIC COMPANY | ) | Docket Nos. 50-274 OL |
| | ) | 50-323 OL |
| (Diablo Canyon Nuclear Power Plant Units 1 and 2) | ) | |

AFFIDAVIT OF FAUST ROSA REGARDING
RESIDUAL HEAT REMOVAL SYSTEM

I, Faust Rosa being duly sworn, state as follows:

1. I am employed by the U.S. Nuclear Regulatory Commission as Chief, Instrumentation and Control Systems Branch, Division of Systems Integration, Office of Nuclear Reactor Regulation.

2. I have reviewed the Joint Intervenor's Motion to Augment or, in the alternative, to reopen the record, dated February 14, 1984, and John H. Cooper's affidavit of January 19, 1984 attached thereto, concerning perceived deficiencies in the design of the Diablo Canyon Residual Heat Removal System.

3. Mr. Cooper's affidavit concerning perceived deficiencies in the design of the Diablo Canyon Residual Heat Removal System is essentially a reiteration of his concerns documented in Allegations No. 37 through 45 and 177 with a few new items not previously addressed. My technical evaluation of his affidavit is limited to the following three areas involving the instrumentation, controls and electric power design of the Residual Heat Removal System:

(a) The use of relays and power supplies in the solid state protection system (SSPS) to provide the automatic closure feature for the residual heat removal (RHR) system isolation valves whenever the reactor coolant system (RCS) pressure exceeds a pre-determined setpoint.

(b) Non-conformance of the design to the recommendation of Regulatory Guide (RG) 1.139 in regard to failure of a power supply causing a change in valve position.

(c) The lack of control room annunciation or alarm of loss of RHR system flow.

None of the foregoing matters raises a concern regarding design quality assurance.

4. Mr. Cooper's Concern

Pages 1, 6 and 121 (Pg. 2 of Exhibit 17B) of Mr. Cooper's affidavit reflect his view that the use of relays and power supplies in the SSPS to effect automatic closure of the RHR isolation valves whenever RCS pressure exceeds a pre-determined setpoint is unnecessary and should be eliminated; the design is such that loss of the SSPS power supply will cause an unwanted automatic closure of an isolation valve with consequent eventual RHR pump damage assuming no operator action. The valves referred to are motor operated valves (MOV) 8701 and 8702.

Relevant Allegation Number

Allegation No. 37.

Staff Response

The original staff response to Allegation No. 37 was provided in Supplement 21 of the Diablo Canyon Safety Evaluation Report (NUREG-0675). This affidavit is intended to supplement the original response to this allegation.

It is my understanding that the automatic closure feature and the prevent opening interlock for the RHR isolation valves are as described in Amendment 4 of the Diablo Canyon FSAR, Section 7.6.2, Residual Heat Removal Isolation Valves. This section of the FSAR is provided as Attachment 1 to this affidavit. Mr. Cooper's concern is with the detailed implementation of the automatic closure feature.

As described by Mr. Cooper, the initiating signals for automatic closure originate in RCS pressure instrument bistable modules (also referred to as signal comparators). Thus, for each valve, one of these signals is input to the SSPS where it energizes an input relay; a contact from this relay is used to energize, using an SSPS power source, an auxiliary relay located in a engineered safeguards cabinet; and a contact from this auxiliary relay is in turn used to initiate the closure circuitry in the motor controller of the isolation valve.

It should be noted that the diverse automatic closure signal (pressurizer steam space temperature, for one valve only, see Attachment 1) is incorporated into the signal from an RCS pressure bistable before this signal leaves the instrumentation cabinet. Therefore, this aspect of the automatic closure design is not relevant to Mr. Cooper's concern.

As stated in the staff response to Allegation No. 37, the automatic closure circuit is designed to "fail safe" on loss of power, i.e., to initiate closure of its associated isolation valve should loss of control power occur. This is required by General Design Criterion (GDC) 23, Protection System Failure Modes; which states:

> "The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air) or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced."

The principal safety function of the RHR isolation valves is to protect the RHR system from overpressure and possible consequent LOCA outside containment. The principal safe state for these valves, therefore, is closed. Thus, the loss of any one of three control power sources: (1) the SSPS power used to energize the auxiliary relay, (2) the power feed to the RCS pressure instrument, or (3) the power feed to the pressurizer steam space temperature instrument (for one valve), will automatically close an isolation valve. Also, in order to meet the channel/train independence requirements of IEEE Std. 279-1971, for each valve, all three power feeds should originate from an independent inverter supplied vital

instrument bus. It is my understanding that the design has been implemented in this manner. Thus, the loss of either one of two vital instrument buses would automatically close an isolation valve. As long as the fail safe feature is retained, this automatic closure would occur on loss of control power regardless of its source.

It should be noted that the RHR design does not provide automatic closure of the isolation valves on loss of actuation power. This is because MOV's inherently fail "as is" on loss of actuation power. Thus, they will remain closed, i.e., in the safe position, if actuation power is lost when they are actually performing their principal protection function. The fact that the isolation valves will remain open if the power failure occurs during the cooling mode is also acceptable for the following reasons: (1) a RCS pressure transient requiring closure of the isolation valves concurrent with or immediately following a loss of actuation power is a very unlikely event, (2) redundant sources of actuation power (offsite and onsite emergency power) are available for each valve, and (3) the control and instrument power for each valve is an independent battery backed inverter so that, given the loss of both the offsite and onsite actuation power for one valve, the other valve would have its independent onsite actuation power available and its independent automatic closure circuitry available to close the valve if this was needed for protection against an RCS pressure transient. Therefore, in my judgement, the overall instrumentation, control and actuation power design of the RHR isolation

valves is in full conformance with the requirements of GDC 23, provides sufficient assurance of RHR decay heat removal capability and RHR system overpressure protection, and is, therefore, acceptable.

I have no direct knowledge of the specific considerations involved in the decision to use SSPS input relays and power sources to implement the automatic closure function. It obviously could have been implemented differently. It is noted, however, that the SSPS is the point where the transition from protection instrumentation channel(s) output to protection system train(s) input normally occurs, and from which the train oriented protection actuation signals normally originate, for most safety-related functions. This is true for the reactor trip and all engineered safeguards actuation functions. The automatic RHR isolation valve closure circuits are safety-related and redundant, and include instrument channel inputs and train oriented actuation signal outputs. Therefore, I believe that the SSPS was used in order to meet the channel/train separation and independence requirements in a manner consistent with the general design used for implementing these requirements for essentially all the protection system functions.

Conclusion

The design of the automatic closure circuitry for the RHR isolation valves meets the applicable regulatory requirements for safety-related systems; these include the "fail safe" feature required by

GDC-23, Protection System Failure Modes, and the requirements for protection channel/train independence and separation of IEEE Std. 279-1971, Criteria for Protection Systems for Nuclear Power Generating Station (10 CFR 50.55h). Therefore, I find the design acceptable.

5. Mr. Cooper's Concern

Page 8 of Mr. Cooper's affidavit cites the lack of conformance of the design of the Diablo Canyon RHR system to the guidance provided by Regulatory Guide 1.139, Guidance For Residual Heat Removal. In the area of instrumentation and controls, he states that "The Diablo Canyon RHR system does not meet the criterion that "Failure of a power supply should not cause any valve to change position"."

Relevant Allegation

None.

Staff Response

The above cited "criterion" is taken from Position 2.a of proposed R.G. 1.139 dated May 1978. This version of the guide was issued for public comment. Subsequently, a draft Revision 1 (dated June 1980) of this proposed guide was prepared by the staff. In this revision the guidance regarding power supply failure reads as follows: "Upon loss of actuating power, (emphasis added) isolation valves should not change position unless movement is to a position that provides

greater safety." Neither version is consistent with GDC-23 which requires a fail safe design on loss of power without qualification as to whether it is control or actuation power that is lost (See the staff response in Item 4 of this affidavit.); the original version of the guide does not specify a fail safe design, while Revision 1 specifies a fail safe design only for loss of actuation power.

However, neither the original version or Revision 1 of this guide was officially issued by the NRC. Therefore, this guide does not reflect Commission policy or guidance and is not used by the staff in the review process. Further development of this guide is now deferred pending completion of Unresolved Safety Issue, TAP A-45, Shutdown Decay Heat Removal Requirements. Diablo Canyon will be subject to any new requirements relating to instrumentation, control and electric power that may result from the work of TAP A-45.

The acceptability of the existing RHR system design in this area for assuring plant safety is discussed in Items 4 and 6 of this affidavit.

Conclusion

The regulatory guide cited by Mr. Cooper has not been officially issued by the NRC and is, therefore, not applicable to the evaluation of the design of the RHR system. The principal criteria used by the staff for this purpose in the area of instrumentation and controls are GDC-23 and IEEE Std. 279, as stated in Item 4 of this affidavit.

6. Mr. Cooper's Concern

Pages 6 and 123 (Pg. 4 of Exhibit 17B) of Mr. Cooper's affidavit reflect his view that an RHR system loss of flow alarm should be provided in the control room immediately.

Relevant Allegation

Allegation No. 39.

Staff Response

As stated in the staff response to Allegation No. 39, the licensee was required to install a loss of RHR system flow alarm in the control room during the first refueling. The staff found this acceptable based on the following considerations which in aggregate provide a high degree of assurance of decay heat removal capability: (1) the presently available control room indications of loss of decay heat removal and RHR system status, (2) the time available for the operator to take corrective action following a spurious RHR system isolation, (3) the alternate means available for decay heat removal in event the RHR system is inoperable, and (4) the technical specification requirements that provide assurance of sufficient decay heat removal capability.

The licensee has since committed to install a RHR low flow alarm prior to entry into Mode 1 operation (PG and E Letter No. DCL-84-057 to G. W. Knighton (NRC) dated February 15, 1984). The licensee has also identified and described the administrative controls and procedures which are in effect and which govern the removal of power from the RHR isolation valves (MOV's 8701 and 8702) by opening the associated breakers; this will be done with the valves closed in operating Modes 1 through 3 and with the valves open in Modes 4 through 6. We have established that opening these breakers will not deenergize the valve position indication lights in the control room.

The removal of power from these valves has been evaluated from the standpoint of operator ability to conduct a plant cooldown from the control room and found acceptable; this evaluation is provided in Item 5 of the affidavit filed by Mr. Chu-Yu Liang of the NRC staff. The accelerated installation of the low flow alarm and the removal of power from MOV's 8701 and 8702 during RHR cooling should effect a substantial reduction in the vulnerability of the RHR pumps to damage due to spurious closure of the isolation valves.

It is noted that opening the isolation valve breakers during RHR cooling defeats the automatic closure overpressure protection for the RHR system. However, after installation of the RHR low flow alarm, the staff will require that these breakers remain closed, thus, the automatic closure feature will be reinstated. In the interim, the RHR safety relief valves, and the plant and RHR system status indications and alarms available in the control room coupled with the administrative controls in effect during RHR cooling, provide sufficient assurance that overpressurization of the RHR system will not occur.

Conclusion

In the interim before installation of the RHR system low flow alarm in the control room prior to initial operation in Mode 1, the existing control room status indications and alarms and the existing procedures are sufficient to assure adequate decay heat removal capability, and in conjunction with the RHR safety relief valves, will also provide adequate protection against overpressurization of the RHR system.

7. Overall Summary

Mr. Cooper has raised a number of concerns regarding the adequacy of the instrumentation and controls design for the Diablo Canyon RHR system. The Staff has addressed these concerns in its response to Allegations No. 37 and No. 39, and in the discussions provided above in this affidavit.

In summary, the Staff concludes that: (1) the design of the automatic closure circuitry for the RHR isolation valves is acceptable, based on its conformance to the applicable regulatory criteria (GDC-23 and IEEE Std. 279); (2) the citation of R.G. 1.139 by Mr. Cooper to support his position that loss of control power should not result in isolation valve closure is not valid because this proposed guide was not formally issued and does not reflect official Commission policy or guidance; and (3) the existing design, procedures, and control room indications and alarms provide sufficient assurance of decay heat removal capability and RHR system overpressure protection during the interim until the RHR low flow alarm is installed prior to initial entry into Mode 1 operation.

The above statements and opinions are true and correct to the best of my knowledge and belief.

Faust Rosa

Faust Rosa

Subscribed and sworn to before me
this 15th day of March 1984

Claire C. Hewitt
Notary Public

My commission expires July 1, 1986

## 7.6.2 RESIDUAL HEAT REMOVAL ISOLATION VALVES

### Description

There are two motor operated gate valves in series in the inlet line from the Reactor Coolant System to the Residual Heat Removal System. They are normally closed and are only opened for residual heat removal after system pressure is reduced below approximately 400 psig and system temperature has been reduced to approximately 350°F. (See Chapter 5 for details of the Residual Heat Removal System). They are the same type of valve and motor operator as those used for accumulator isolation, but they differ in their controls and indications in the following respect:

1. One isolation valve, that nearest the Reactor Coolant System, is interlocked with a pressure signal to prevent its being opened whenever the system pressure is greater than 425 psig. The valve will also be closed automatically whenever the system pressure increases above approximately 600 psig. This interlock and automatic closing action is derived from one process control channel.

2. The other valve, that nearest the Residual Heat Removal System, is similarly interlocked and automatically controlled. Control signals are derived from a second process control channel. In order to comply with IEE-279 and to provide diversity, this valve will also be prevented from opening when the pressurizer vapor space temperature exceeds approximately 455°F and automatically closed when the pressurizer vapor space temperature exceeds approximately 490°F. This temperature control signal is derived from one process instrumentation protection channel. 4

### Analysis

Based on the scope definitions presented in Reference 2 (IEEE-279), 1971) and Reference 3 (IEEE-338, 1971), these criteria do not apply to the residual heat removal isolation valve interlocks; however, in order to meet AEC requirements and because of the possible severity of the consequences of loss of function, the requirements of IEEE-279 will be applied with the following comments.

1. For the purpose of applying IEEE-279, 1971, to this circuit, the following definitions will be used.

   a. Protection System

      The two valves in series in each line and all components of their interlocking and closure circuits.

   b. Protective Action

      The automatic initiation and maintenance of Residual Heat Removal System isolation from the Reactor Coolant System pressures above redidual heat removal design pressure.

2. IEEE-279, Paragraph 4.10: The requirement for on-line test and calibration capability is applicable only to the actuation signal and not to the isolation valves, which are required to remain closed during power operation.

3. IEEE-279, Paragraph 4.15: This requirement does not apply, as the setpoints are independent of mode of operation and are not changed.

Environmental qualification of the valves and wiring are discussed in Section 3.11.

7.6.3 REFUELING INTERLOCKS

Electrical interlocks (i.e., limit switches) are provided for minimizing the possibility of damage to the fuel during fuel handling operations. Mechanical stops are provided as the primary means of preventing fuel handling accidents. For example, safety aspects of the manipulator crane depends on the use of electrical interlocks and

FAUST ROSA

PROFESSIONAL QUALIFICATIONS

INSTRUMENTATION AND CONTROL SYSTEMS BRANCH

DIVISION OF SYSTEMS INTEGRATION

I have been employed by the Nuclear Regulatory Commission since January 1971. From January 1977 through 1980 I served as Chief, Power Systems Branch, and since January 1981 as Chief, Instrumentation and Control Systems Branch, both branches being in the Division of Systems Integration. Prior to these assignments, I served as a Section Chief in the Electrical, Instrumentation and Control Systems Branch, Division of Systems Safety, and in the Plant Systems Branch, Division of Operating Reactors. I have participated in the review of instrumentation, control and electrical systems of numerous nuclear power stations and in the formulation of related standards and Regulatory Guides.

The Instrumentation and Control Systems Branch performs an in-depth technical review of the design and operation of nuclear power plant instrumentation and control systems important to safety including: protection systems, engineered safety feature control systems, safe shutdown systems, information systems, interlock systems, plant control systems and essential auxiliary supporting systems. This review includes a comprehensive assessment of these systems for all power reactors for adherence to appropriate codes and standards and encompasses complete evaluation of applicant's safety analysis reports, generic reports, and other related system design information. Further, the Branch develops the bases for Regulatory acceptance criteria for instrumentation and control systems designs; evaluates experience obtained during the construction

and operation of nuclear power plants and relates this information to future evaluations and acceptance criteria; and participates in the development of Regulatory Guides and regulations pertaining to instrumentation and control systems important to safety.

The Power Systems Branch performs comparable reviews, evaluations and criteria development functions primarily in the area of electric power systems important to safety.

I hold a Bachelor of Electrical Engineering degree from the University of Pittsburgh, Pittsburgh, Pennsylvania. In addition, I have taken courses in Mathematics, Theoretical Physics, Nuclear Physics and Engineering, and Radiation Shielding at the University of Pittsburgh and at the Reactor School of the Bettis Atomic Power Laboratory, Westinghouse Electric Corporation.

My nuclear engineering experience background derives from my employment at the Bettis Atomic Power Laboratory of Westinghouse Electric Corporation, West Mifflin, Pennsylvania, from May 1955 to September 1962; and from my employment at the Bechtel Corporation, Vernon, California, from September 1969 to January 1971. At Bettis Laboratory I was a lead engineer in the nuclear submarine power plant group with technical responsibility for nuclear instrumentation, rod control, and reactor protection systems. Work involved component and system design, installation, testing, modification and documentation. I also served as Bettis representative during full-scale tests conducted by the Navy. At Bechtel I conducted engineering studies and prepared

reports and specifications relating to the design and construction of the Rancho Seco Nuclear Power Station. This work was primarily in the areas of safety-related electrical power, instrumentation and control systems.

My non-nuclear engineering background derives primarily from my employment in the Construction Engineering Department of the National Tube Company, United States Steel Corporation, Lorain, Ohio, from June 1947 to April 1955; and from my employment at the Rocketdyne Division of North American Rockwell Corporation, Canoga Park, California, from October 1962 to March 1968. At National Tube I served as a Senior Engineer engaged in design and development of electrical power and control systems for new pipe mills from conceptual design through detail design, procurement, installation, and initial operation. This work extended through completion of two major pipe mill construction projects. At Rocketdyne I was a Research Specialist engaged in design and development of controls and instrumentation for a dual turbo-pump liquid hydrogen feed system for a nuclear rocket engine. My primary responsibility was for control system integration extending from conceptual design through procurement, installation, and completion of the test program.

I am a member of the Institute of Electrical and Electronic Engineers and have served on its Standards Board. I have participated in the nuclear standards development work of this organization since 1972.

I am a registered Electrical Engineer in the State of Ohio, Registration No. E-020166.