

50-323

ENCLOSURE 2

SAFEGUARDS SAFETY EVALUATION REPORT

DIABLO CANYON NUCLEAR POWER STATION

UNIT 2

8609250067 860905
PDR FOIA
HOLMES86-197 PDR

1.0 Introduction

The Pacific Gas and Electric Company filed with the Nuclear Regulatory Commission for the Diablo Canyon Nuclear Power Station physical security, safeguards contingency, and guard training and qualification plans.

This Safety Evaluation Report (SER) summarizes how the licensee has provided for meeting the requirements of 10 CFR Part 73. The SER is composed of a basic analysis that is available for public review, and a protected Appendix.

2.0 Physical Security Organization

To satisfy the requirements of 10 CFR 73.55(b) the Pacific Gas and Electric Company has provided a physical security organization that includes a Shift Security Supervisor who is on-site at all times with the authority to direct the physical protection activities. To implement the commitments made in the physical security plan, training and qualification plan, and the safeguards contingency plan, written security procedures specifying the duties of the security organization members have been developed and are available for inspection.

The training program and critical security tasks and duties for the security organization personnel are defined in the "Diablo Canyon Nuclear Power Station Training and Qualification Plan" which meets the requirements of 10 CFR Part 73, Appendix B for the training, equipping and qualification of the security organization members. The physical security plan and the training program provide commitments that preclude the assignment of any individual to a security related duty or task prior to the individual being trained, equipped and qualified to perform the assigned duty in accordance with the approved guard training and qualification plan.

3.0 Physical Barriers

In meeting the requirements of 10 CFR 73.55(c) the applicant has provided a protected area barrier which meets the definition in 10 CFR 73.2(f)(1). A 20 foot wide isolation zone, to permit observation of activities at the perimeter, is provided (except for the locations listed in the Appendix) along both sides of barrier.

The staff has reviewed those locations and determined that the security measures in place are satisfactory and continue to meet the requirements of 10 CFR 73.55(c).

Illumination of 0.2 foot-candles is maintained for the isolation zones, protected area barriers, and external portions of the protected area.

4.0 Identification of Vital Areas

The Appendix contains a discussion of the applicant's vital area program and identifies those areas and items of equipment determined to be vital for protection purposes. Vital equipment is located within vital areas which are located within the protected area and which require passage through at least two barriers, as defined in 10 CFR 73.2(f)(1) and (2), to gain access to the vital equipment (except as noted in the Appendix). Vital area barriers are separated from the protected area barrier.

The control room and central alarm station are provided with bullet-resistant walls, doors, ceilings, floors, and windows. Based on these findings and the analysis set forth in paragraph C of the Appendix, the staff has concluded that the applicant's program for identification and protection of vital equipment satisfies the regulatory intent. However, this program is subject to on-site validation by the staff in the future, and to subsequent changes if found to be necessary.

5.0 Access Requirements

In accordance with 10 CFR 73.55(d) all points of personnel and vehicle access to the protected area are controlled. The individual responsible for controlling the final point of access into the protected area is located in a bullet-resistant structure. As part of the access control program, vehicles (except under emergency conditions), personnel, packages, and materials entering the protected area are searched for

explosives, firearms and incendiary devices by electronic search equipment and/or physical search.

Vehicles admitted to the protected area, except licensee designated vehicles, are controlled by escorts when in operation. Licensee designated vehicles are limited to on-site station functions and remain in the protected area except for operational maintenance, repair, security and emergency purposes. Positive control over the vehicles is maintained by personnel authorized to use the vehicles or by the escort personnel. A picture badge/key card system, utilizing encoded information, identifies individuals that are authorized unescorted access to protected and vital areas, and is used to control access to these areas. Individuals not authorized unescorted access are issued non-picture badges that indicate an escort is required. Access authorizations are limited to those individuals who have a need for access to perform their duties.

Unoccupied vital areas are locked and alarmed. During periods of refueling or major maintenance, access to the reactor containment is positively controlled by a member of the security organization to assure that only authorized individuals and materials are permitted to enter. In addition, all doors and personnel/equipment hatches into the reactor containment are locked and alarmed. Keys, locks,

combinations and related equipment are changed on an annual basis. In addition, when an individual's access authorization has been terminated due to the lack of reliability or trustworthiness, or for poor work performance, the keys, locks, combinations and related equipment to which that person had access are changed.

6.0 Detection Aids

In satisfying the requirements of 10 CFR 73.55(e) the applicant has installed intrusion detection systems at the protected area barrier, at entrances to vital areas, and at all emergency exits. Alarms from the intrusion detection system announce within the continuously manned central alarm station and a secondary alarm station located within the protected area. The central alarm station is located such that the interior of the station is not visible from outside the perimeter of the protected area. In addition, the central alarm station is constructed so that walls, floors, ceilings, doors, and windows are bullet-resistant. The alarm stations are located and designed in such a manner so a single act cannot interdict the capability of calling for assistance or responding to alarms. The central alarm station contains no other functions or duties that would interfere with its alarm response function. The intrusion detection system transmission lines and associated alarm

annunciation hardware are self-checking and tamper-indicating. Alarm annunciators indicate the type of alarm and its location when activated. An automatic indication of when the alarm system is on standby power is provided in the central alarm station.

7.0 Communications

As required in 10 CFR 73.55(f) the applicant has provided for the capability of continuous communications between the central and secondary alarm station operators, guards, watchmen, and armed response personnel through the use of a conventional telephone system, and a security radio system. In addition, direct communication with the local law enforcement authorities is maintained through the use of a conventional telephone system and two-way VHF radio links. All non-portable communication links, except the conventional telephone system, are provided with an uninterruptable emergency power source.

8.0 Test and Maintenance Requirements

In meeting the requirements of 10 CFR 73.55(g) the applicant has established a program for the testing and maintenance of all intrusion alarms, emergency alarms, communication equipment, physical barriers and other security related devices and equipment. Equipment or devices that do not meet the design performance criteria or have failed to otherwise operate will be compensated for by appropriate compensatory measures as defined in the "Diablo Canyon Nuclear Power Station Physical Security Plan" and in site procedures. The compensatory

measures defined in these plans will assure that the effectiveness of the security system is not reduced by failures or other contingencies affecting the operation of the security related equipment or structures. Intrusion detection systems are tested for proper performance at the beginning and end of any period that they are used for security. Such testing will be conducted at least once every seven days.

Communication systems for on-site communications are tested at the beginning of each security shift. Offsite communications are tested at least once each day.

Audits of the security program are conducted once every 12 months by personnel independent of site security management and supervision. The audits, focusing on the effectiveness of the physical protection provided by the on-site security organization implementing the approved security program plans, include, but are not limited to: a review of the security procedures and practices; system testing and maintenance programs; and local law enforcement assistance agreements. A report is prepared documenting audit findings and recommendations and is submitted to the plant management.

9.0 Response Requirements

In meeting the requirements of 10 CFR 73.55(h) the applicant has provided for armed responders immediately available for response duties on all shifts consistent with the requirements of the regulations. Considerations used in support of this

number are attached (see Appendix). In addition, liaison with local law enforcement authorities to provide additional response support in the event of security events has been established and documented.

The applicant's safeguards contingency plan for dealing with thefts, threats and radiological sabotage events satisfies the requirements of 10 CFR Part 73, Appendix C. The plan identifies appropriate security events which could initiate a radiological sabotage event and identifies the applicant's preplanning, response resources, safeguards contingency participants and coordination activities for each identified event. Through this plan, upon the detection of abnormal presence or activities within the protected or vital areas, response activities using the available resources would be initiated. The response activities and objectives include the neutralization of the existing threat by requiring the response force members to interpose themselves between the adversary and their objective, instructions to use force commensurate with that used by the adversary, and authority to request sufficient assistance from the local law enforcement authorities to maintain control over the situation.

To assist in the assessment/response activities a closed circuit television system, providing the capability to observe the entire protected area perimeter, isolation

zones and a majority of the protected area, is provided to the security organization.

10.0 Employee Screening Program

In meeting the requirements of 10 CFR 73.55(a) to protect against the design basis threat as stated in 10 CFR 73.1 (a)(1)(ii), the Pacific Gas and Electric Company has provided an employee screening program. Personnel who successfully complete the employee screening program or its equivalent may be granted unescorted access to protected and vital areas at the Diablo Canyon site. All other personnel requiring access to the site are escorted by persons authorized and trained for escort duties and who have successfully completed the employee screening program. The employee screening program is based upon accepted industry standards and includes a background investigation, a psychological evaluation, and a continuing observation program. In addition, the applicant may recognize the screening program of other nuclear utilities or contractors based upon a comparability review conducted by the Pacific Gas and Electric Company. The plan also provides for a "grandfather clause" exclusion which allows recognition of a certain period of trustworthy service with the utility or contractor, as being equivalent to the overall employee screening program. The staff has reviewed the applicant's screening program against the accepted industry standards (ANSI N13.17 1973) and has determined that the program is acceptable.

SALP INPUT EVALUATION
DIABLO CANYON SAFEGUARDS REVIEW

<u>Criteria</u>	<u>Category</u>
1. <u>Management Involvement and Control in Assuring Quality</u> The applicant has provided consistent evidence of prior planning and assignment of priorities. Decision making is consistently at a level that ensures adequate management review.	1
2. <u>Approach to Resolution of Technical Issues from a Safety Standpoint</u> The applicant has provided technically sound, timely, and thorough approaches in almost all cases.	1
3. <u>Responsiveness to NRC Initiatives</u> The applicant provides timely, acceptable resolutions of issues.	1
4. <u>Enforcement History</u>	N/A
5. <u>Reporting of Reportable Events</u>	N/A
6. <u>Staffing (Including Management)</u> Positions are identified, authorities and responsibilities are well defined.	1
7. <u>Training and Qualification Effectiveness</u> The safeguards training and qualification plan and procedures contribute to a well defined security program.	1



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

M. Mendonca
S. Resident Diablo

JAN 28 1985

Marc, this is
internal, do not
share with PG&E

MEMORANDUM FOR: RSB Members

FROM: Brian W. Sheron, Chief
Reactor Systems Branch, DSI

SUBJECT: AUTO CLOSURE INTERLOCKS FOR PWR RESIDUAL HEAT
REMOVAL (RHR) SYSTEMS

1 Jan
492 7100

The purpose of this memo is to bring all RSB members up to date on recent decisions and issues regarding PWR RHR systems open permissive interlocks (OPI) and auto closure interlocks (ACI), and to set forth some preliminary guidelines for evaluating proposed changes.

Background

The Standard Review Plan Chapter for PWR RHR systems, SRP 5.4.7, contains Branch Technical Position RSB 5-1 that sets forth acceptable means of providing RHR system isolation. In particular, paragraphs B.1.b and B.1.c state, for the suction side isolation valves (i.e., valves between the RCS and the RHR pump suction):

"The valves shall have independent diverse interlocks to prevent the valves from being opened unless the RCS pressure is below the RHR system design pressure. Failure of a power supply shall not cause any valve to change position."

"The valves shall have independent diverse interlocks to protect against one or both valves being open during an RCS increase above the design pressure of the RHR system."

The positions have traditionally been met for plants under review or licensed since RSB BTP 5-1 became effective in 1978 by a set of circuits that prohibit suction valve opening until RCS pressure is below the RHR design pressure and initiate automatic suction valve closure when RCS pressure rises above the RHR design pressure. The suction isolation valves are never commanded to automatically open.*

CONTACT: W. Jensen, RSB
X29406

* Only the RHR suction valves to the RWST or to the containment sump must function during the injection (automatically) and recirculation (manually or automatically) phases of a design basis accident.

~~850206055T~~
6pp.

WMB/24
[Signature]

JAN 28 1900

RSB Members

- 2 -

The purposes of the OPI and ACI are basically the same--to prevent a LOCA outside containment, (event V per WASH-1400). The OPI is intended to ensure that while the RCS is at full pressure, the RHR suction valves cannot be opened. Although safety relief valves are located on the suction piping, these valves would not be capable of preventing the RHR system from being pressurized beyond its design pressure if the system were suddenly subjected to full RCS pressure.*

The ACI is also intended to prevent Event V LOCA, but during a different scenario. During a RCS startup from modes where the RHR system has been utilized, the operating procedures call for closure of the RHR suction valves before RCS pressure reaches the RHR safety relief valve (SRV) setpoint.** If the operator failed to close both suction isolation valves, then, absent ACIs, the SRVs would lift. Startup could not proceed as the SRV is generally sufficiently sized to prevent further pressurization. With the ACIs, operator error in failing to close both valves would not prevent startup since the ACI is generally, although not always, set at a pressure below the SRV setpoints.

In the absence of the ACI, if the operator closes only one suction isolation valve and thus is able to continue the startup, a subsequent failure of the single closed isolation valve would lead to an Event V. The purpose of the ACI is to close, or to provide a backup to the operator to close the second suction isolation valve.

With or without the ACI, there must be a valve mechanical failure (i.e., the gate failing in such a way that the valve's isolation capability is lost) or a hot short, (i.e., that electrically actuates the valve to open) for the Event V to occur. The ACI is intended to reduce the probability of an Event V by backing up the operator in closing both isolation valves.

The ASME code (Section NB 3412.4) requires the open-permissive interlocks but does not require the auto closure interlocks.

* It is not known if the suction valves could even be opened in this scenario, given the high differential pressure acting against the gate valve, and the relatively low motor torque.

** The intent is to prevent the SRV from lifting causing loss of coolant into the containment sump and the possibility that the SRV will not reset.

JAN 28 1985

Fire Protection Reviews

In the course of performing the fire protection reviews in accordance with 10 CFR 50.48 and Appendix R, the Auxiliary Systems Branch became concerned that a fire located in the control room or other plant areas could cause fire damage which results in hot shorts. These shorts could then result in the RHR suction valves opening and causing an Event V. To remedy this concern, ASB has allowed PWR applicants and licensees to open at least one RHR isolation valve motor power supply breaker when in Modes 1, 2 and 3. Although this alleviates the fire protection concern, it has created two other potential non-conformances with BTP RSB 5-1: (1) the plant is no longer capable of being brought to the cold shutdown condition from inside the control room and (2) the failure to meet the position regarding the ACI, as described above.

The first issue has been addressed for only a few NTOL plants and has been resolved on a case-by-case basis by granting exceptions to BTP RSB 5-1 position. Two PWR applicants have shown that there is reasonable time for operators to go to the motor control center (MCC), rack in the RHR suction valve motor power supply breakers and change the valve's position. Also, these applicants have shown that there would be no severe environments through which the operators would have to pass to get to the MCC and return to the control room.

The second issue is just now coming to light. By allowing power to be removed from the suction valve motors when the reactor is in Modes 1, 2, and 3, the functional capability of the ACI may be defeated. That is, if the operator in the course of starting up the plant, shuts only one suction valve while pressure is below the ACI setpoint, then removes power from both valves to meet the fire protection requirements, the ACI would not be capable of initiating valve motion to close the open valve when pressure reached the ACI setpoint.

RHR Pump Damage and LTOPS

There are other issues related to the RHR system ACI. The industry in general seems to believe that the ACI is detrimental to safety. This belief arises from operational experience. There have been at least 26 events where RHR systems have been inadvertently isolated.* A large fraction of these events have been caused by the ACI shutting the suction valves due to an equipment malfunction or improper testing.

The inadvertent closure of the RHR suction valve(s) can have adverse consequences. First, it is the system used for removing decay heat when cold shutdown is initiated. Although the expected RCS heatup rate would be low due to the low decay heat levels when the RHR system is in use, if the suction

* EPRI, NSAC-52, Residual Heat Removal Experience Review and Safety Analysis.

JAN 28 1985

RSB Members

- 4 -

valve can not be reopened, other means of decay heat removal would have to be established (e.g., steam generators). Depending on the plant condition, these other methods may be difficult to achieve.

Second, the RHR pumps may be destroyed without prompt operator actions. Events at Calvert Cliffs and Diablo Canyon have resulted in destruction of at least one of the RHR pumps due to cavitation and loss of bearing cooling.

Third, if the RCS is in a water solid condition, loss of RHR flow will result in a pressure transient since the charging pumps would be injecting into the RCS without any letdown flow. Although there are systems currently provided on all PWRs to mitigate this event (i.e. Low Temperature Overpressure Protection Systems-LTOPS), there have been a number of transients initiated by inadvertent closure of the RHR isolation valves.

Kewaunee and Diablo Canyon

Two plants have recently requested alterations in their RHR suction valve control circuitry that have forced the staff to consider the overall benefits and detriments of the ACI in light of the fire protection reviews and industry experience. Kewaunee is a two loop W PWR with two RHR drop lines. In December, 1983, the licensee requested complete removal of their ACIs. The utility believes that the ACI presents a high potential for inadvertent RHR isolation and, for Kewaunee, a loss of the LTOP system.

A study conducted by Westinghouse to support the proposed change shows that removal of the ACI, for Kewaunee, would be a safety improvement in that the scenarios that result in low temperature overpressure transients would not be accompanied by RHR isolation, nor would the RHR system be overpressurized. The licensee has proposed three means of preventing Event V: (1) alarms to indicate if a RHR isolation valve is not closed, (2) rewiring the motor control switches to close, but not open, both valves when one button is depressed, and (3) operating procedures that ensure all RHR MOVs are closed during reactor startups. The staff's review of the Kewaunee proposal is complete and has concluded that the Kewaunee proposal is acceptable.

Diablo Canyon is a four loop W PWR with only a single RHR drop line. As a result of allegations made during the licensing process, the staff reviewed the RHR isolation valve operating procedures and found that the licensee should retain power available to the MOVs when the RHR system is in operation. Previously, the licensee removed power from these valves when the RHR system was in use since a spurious RHR ACI actuation resulted in a loss of RHR suction and damage to the RHR pumps.

JAN 28 1985

RSB Members

- 5 -

The licensee has modified its procedures to require power to be available to the RHR valves, but has subsequently requested that the staff permit power to be removed from the valves. The staff is now requesting the licensee to address the possibility of removal of the ACI, since this is, in fact, the root cause of inadvertent closures, not the availability of power to the isolation valves. If the ACIs were removed and an alarm installed to warn the operators should either of the two MOVs be in the incorrect position, protection from Event V could be provided and inadvertent closure would be prevented. The review of the Diablo Canyon proposal has led to another concern: if power is removed from the RHR MOVs to remove the possibility of an inadvertent closure, then no ready means would be available to isolate the RHR system should it rupture or develop a leak outside containment. The proposed removal of power from the RHR MOVs for Diablo Canyon is, in essence, caused by the various problems cited by Kewaunee and the industry as a whole regarding the ACI.

RSB Position

The issue of RHR ACI reliability is being prioritized by SPEB. In the meantime, proposals to change the RHR system isolation valve controls should be carefully considered, especially in light of the many overlapping concerns.

There is no reason, as yet, to allow or even encourage whole scale removal of the ACI. The request by each plant should be reviewed on a case-by-case basis. As a minimum, however, any proposal to remove the ACI should be substantiated by proof that the change is a net improvement in safety. For example, requests for removal of power or the ACI should assess as a minimum, the following:

1. The means available to minimize Event V concerns.
2. The alarms to alert the operator of an improperly positioned RHR MOV.
3. The RHR relief valve capacity must be adequate.
4. Means other than the ACI to ensure both MOVs are closed (e.g., single switch actuating both valves).

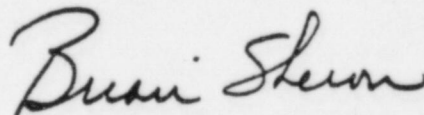
JAN 28 1985

RSB Members

-6-

5. Assurance that the function of the open permissive circuitry is not affected by the proposed change.
6. Assurance that MOV position indication will remain available in the control room, regardless of the proposed change.
7. An assessment of the proposed change's effect on RHR reliability, as well as on LTOPs concerns.

We are conducting our own probabilistic assessment as an adjunct to work being conducted by the industry. This work should be complete within the next few months.



Brian W. Sheron, Chief
Reactor Systems Branch, DSI

cc: R. Bernero ...
R. Houston
T. Speis
D. Eisenhut
W. Minners
H. Vandermolen
O. Parr
J. Wermiel
J. Wilson