NUREG 1286
Supplement No. 1

Safety Evaluation Report

related to the restart of
Rancho Seco Nuclear Generating Station, Unit 1,
following the event of December 26, 1985

Docket No. 50-312

Sacramento Municipal Utility District

U.S. Nuclear Regulatory
Commission

Office of Nuclear Reactor Regulation

March 1988

NOTICE

Availability of Reference Materials Cited in NRC Publications

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

1. The NRC Public Document Room, 1717 H Street, N.W.
   Washington, DC 20555
2. The Superintendent of Documents, U.S. Government Printing Office, Post Office Box 37082,
   Washington, DC 20013-7082
3. The National Technical Information Service, Springfield, VA 22161

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

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

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

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

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

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

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Division of Information Support Services, Distribution Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

NUREG-1286
Supplement No. 1

Safety Evaluation Report

related to the restart of
Rancho Seco Nuclear Generating Station, Unit 1,
following the event of December 26, 1985

Docket No. 50-312

Sacramento Municipal Utility District

U.S. Nuclear Regulatory Commission

Office of Nuclear Reactor Regulation

March 1988

ABSTRACT

On December 26, 1985, the Rancho Seco Nuclear Generating Station experienced a reactor trip from 76% power, followed by a rapid overcooling transient and automatic initiation of the safety features actuation system. The unit has remained shut down since that time. In response to confirmatory letters from the NRC Region V Administrator, the licensee, Sacramento Municipal Utility District (SMUD), submitted the "Rancho Seco Action Plan for Performance Improvement" in July 1986. Since then, the licensee has submitted revisions to that action plan and numerous other documents and information to support a return of Rancho Seco to power operation. The NRC staff reviewed the licensee's submittals and other information made available to the staff in support of a restart of Rancho Seco. In October 1987, the NRC staff issued a Safety Evaluation Report (NUREG-1286) relating to the restart of Rancho Seco. Since then, the staff has completed its review of all other issues relating to the restart effort. The results of this more recently completed review work are contained in this Supplement No. 1 to NUREG-1286 (SSER 1).

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

FIGURES

TABLES

TABLE OF CONTENTS (Continued)

APPENDICES

1 INTRODUCTION AND SUMMARY

The Safety Evaluation Report (SER) related to the restart of Rancho Seco following the December 26, 1985 event was issued in October 1987 (NUREG-1286). In that report the staff (1) documented the resolution of all restart issues that had been resolved at that time, and (2) identified the remaining issues that would need to be resolved before startup. Among those restart issues were some that required additional staff inspection and some that were still being reviewed by the staff. Those issues have since been resolved, together with all other issues that arose during the course of the staff's review. The resolution of those issues is addressed in this Supplement No. 1 to NUREG-1286 (SSER 1).

1.4 Conclusion

All issues known to the staff that require resolution for restart of Rancho Seco have been resolved to the staff's satisfaction. There are no unresolved issues that should be resolved before restart of the plant. The staff concludes that the plant is ready to restart.

2 BACKGROUND

2.3 Summary of Licensee Response

2.3.2 Evaluation of the Plant Performance and Management Improvement Program

Section 2.3 of the restart SER (NUREG-1286), issued in October 1987, contained a discussion and evaluation of the licensee's Plant Performance and Management Improvement Program (PP&MIP). Section 2.3.2 stated that this issue remained open pending verification by the augmented system review and test program (ASRTP) reinspection and by the NRC staff inspection that the problem resolution and tracking portions of the PP&MIP are adequate. This issue has since been resolved. The details and basis for the resolution of this issue are documented in Inspection Report 50-312/87-29, dated January 25, 1988. This issue, evaluation of the Rancho Seco PP&MIP, is therefore closed as a restart item.

3 RESOLUTION OF CONCERNS RELATED TO THE DECEMBER 26, 1985 EVENT

3.1 Issues of Plant Systems, Electrical Systems, and Instrumentation and Control Systems

3.1.2 ICS/NNI System Failure Modes and Effects on Plant Operation

3.1.2.1 Root Cause of the Event

The December 26, 1985 event at Rancho Seco was initiated by the plant's response to the loss of integrated control system (ICS) ±24-V dc power. The loss of ICS ±24-V dc power occurred when the ICS power supply monitor (PSM) provided an automatic trip signal to shunt trip switches (S1 and S2) in the 120-V ac feeder lines to the ±24-V dc power supplies. This caused the switches to open, thus deenergizing the ±24-V dc supplies. The PSM is designed to monitor voltage on the positive and negative 24-V dc buses, and to automatically open switches S1 and S2 (causing a complete loss of ICS ±24-V dc power) if the voltage on either the positive or negative bus drops to 22.0 V dc. Therefore, the root cause of the event focuses on discovering the specific condition(s) that caused the PSM to signal S1 and S2 to open.

During in-plant investigations following the event, the licensee discovered an abnormal voltage drop measured between the positive 24-V dc bus and the input of the associated PSM sensing circuit. The voltage drop was found to be caused by a resistance created by a bad electrical connection in the distribution wiring between the +24-V dc bus and the PSM (the bad connection was external to the PSM module). This led the licensee to conclude that: "The root cause of the loss of ICS power was a manufacturing defect in the installation of wiring within the ICS cabinet," and "the direct cause was identified as the loss of ICS dc power caused by a manufacturing error on a lug improperly installed on a factory prepared wire."

Because the root cause of the December 26, 1985 event at Rancho Seco centers around the PSM, and because the PSM includes several unique design characteristics that partially explain its behavior during the event, the design and operation of the PSM are discussed separately in detail in Section 3.1.2.8, "Power Supply Monitor," of this report. Also discussed in Section 3.1.2.8 are post-event testing of the PSM by the licensee and by an independent laboratory. Part of the testing by the independent laboratory involved detailed inspection of the PSM module, and a determination of the PSM sensitivity to input resistances such as could be caused by bad electrical connections. The test results included identification of a bad electrical connection internal to the PSM module itself that was found to cause unstable PSM operation under certain conditions. This led the staff to conclude that actuation of the ICS PSM on December , 1985 was not caused by a single factor, but was most likely caused by a combination of factors including (1) an actual degraded voltage condition within the ICS dc power distribution system resulting from a poor electrical connection between the +24-V dc bus and the PSM input and (2) a poor electrical connection within the PSM module. The staff further concluded that inherent

design characteristics of the PSM helped to exacerbate the effects of the poor electrical connections internal and external to the PSM. Other possible contributing causes to the event include the failure to recognize precursor indications in the form of control room alarms momentarily actuated by the PSM, and the lack of preventive maintenance with regard to replacement of switches S1 and S2 at the end of their 5-year-guaranteed life.

These conclusions concerning the root cause for the PSM actuation of switches S1 and S2 on December 26, 1985 and the basis for the conclusions are discussed in detail in Section 3.1.2.8 of this report. The discussion includes the effects of resistance in series with the PSM input (such as would be caused by a bad electrical connection) on PSM operation. Although the staff believes the root cause for the December 26, 1985 event at Rancho Seco involves a combination of factors, the major contributing factor appears to be the bad electrical connection between the +24-V dc bus and the PSM input. The bad connection created a resistance. and hence a voltage drop across the resistance, so that the voltage sensed by the PSM approached the 22.0-V dc trip setpoint for actuation of S1 and S2, although the actual bus voltage appears to have remained at its nominal 24-V dc value.

The evaluation that follows addresses the licensee's program to determine (1) the cause for the bad electrical connection, (2) the extent to which bad electrical connections could present a problem within the ICS and non-nuclear instrumentation (NNI) system, and within safety-related systems, and (3) corrective actions taken by the licensee to resolve identified problems.

Evaluation of Licensee's Root Cause Study and Resultant Program

The +24-V dc bus is located in ICS cabinet 3, and the PSM module is located in ICS cabinet 2. Power is routed to the PSM from the bus through ICS cabinet 1. The bad electrical connection identified as a contributing root cause for the December 26, 1985 event was located in ICS cabinet 1. The licensee's engineering report on action item 3A, "ICS Equipment Investigation," dated February 7, 1986, indicated that the bad electrical connection arose from a poor mechanical connection (i.e., crimp) of the ICS dc power distribution wire to its lug. When the wire was lifted, the lug actually fell off the end of the wire. The licensee stated that detailed examination of this connection failure revealed that the conductor had been insufficiently inserted into the lug barrel. This resulted in an inadequate barrel crimp on the conductor strands at the tongue end of the lug, creating a loose, high resistance connection (see Figure 3.17). Further investigation revealed that bad electrical connections also existed in ICS cabinets 3 and 5. The bad connections were due to either poor crimp connections or the use of improperly sized hardware to attach the lugs to the bus work (several screws holding lugs to bus bars were found to be loose).

On the basis of these investigation results, the licensee developed and implemented an Electrical Termination Inspection and Upgrade Program designed to verify the adequacy of other terminations in cabinets supplied by the ICS vendor, Bailey Controls Corporation. The program included the following tasks:

- identification of questionable electrical terminations
- identification of other potential deficiencies inside instrument cabinets and panels

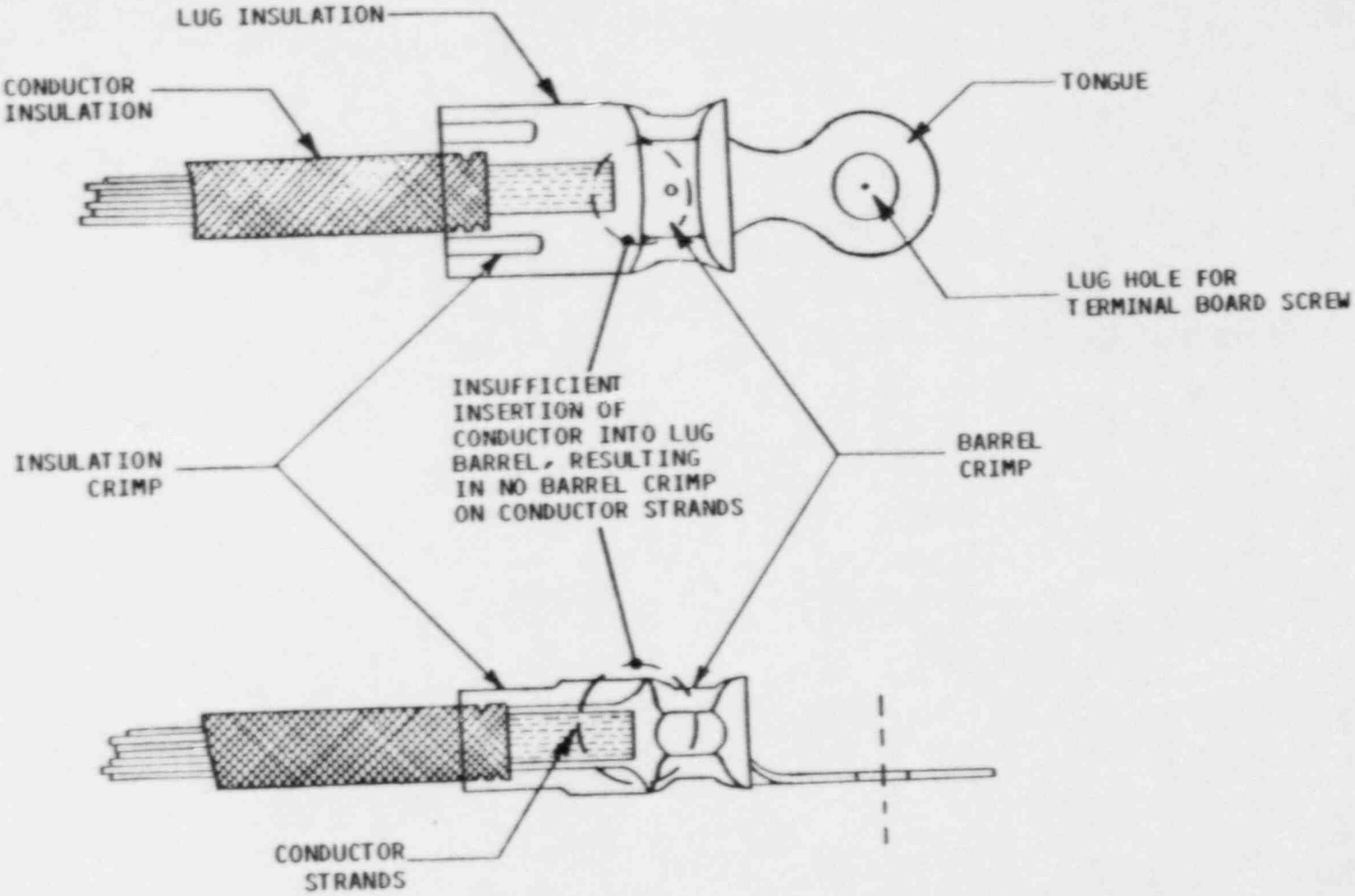


Figure 3.17 December 26, 1985 ICS compression lug termination failure

- correction of all identified deficiencies

- actions to ensure that electrical termination deficiencies do not occur in the future

The initial scope and content of the program consisted of visual inspections of compression lug terminations (both "internal" terminations installed by the vendor in the factory, and "external" terminations installed by the licensee between field wiring and the vendor-supplied cabinets/panels) within the five ICS cabinets and the seven NNI cabinets. The licensee inspected 2250 compression lug terminations within the ICS/NNI cabinets, and identified 2 failures (a failure is defined as a lug termination that becomes disconnected from its conductor during the inspection process) and 950 deviations. Examples of deviations are:

- conductors not visible at the tongue end of the lug barrel

- conductor extends too far beyond the tongue end of the lug barrel so that conductor strands are compressed under the terminal screw

- lug hole too large for terminal screw

- wrong size lug for conductor size

- improperly modified lug

- lugs installed face down (not inspectable)

- lugs bent more than 90 degrees

- lugs twisted or deformed

- more than two lugs on a single stud

- incorrect shield termination

- two lugs under one terminal screw not installed back to back

The licensee has replaced the failed lugs, and either replaced or reworked all identified deviations so that these terminations satisfy the visual inspection criteria.

Because the physical location or orientation (e.g., installed back-to-back or face down) of some compression lug terminations made it impossible to visually inspect them without actually lifting the lugs, the licensee developed "secureness verification" criteria to be used in such situations. Secureness verification testing had the added benefits that safety clearances were not needed (as would be required before lifting certain lugs for visual inspections) and fewer lugs might need replacing (the licensee considered the visual inspection acceptance criteria to be very stringent).

The secureness verification criteria consisted of (1) the ability to withstand a conductor-to-termination pull force of an 8-pound tension for a duration of

1 minute for external terminations and a 2-pound tension for a duration of 1 minute for internal terminations and (2) an electrical function test (performed after the pull-force test) to verify that the maximum measured resistance between the conductor wire and a point on the lug tongue adjacent to the lug barrel did not exceed 0.004 ohm. The licensee believes the 8-pound pull force for external terminations and the 2-pound pull force for internal terminations conservatively bounds the force that any one conductor might be subjected to in the plant's operating environment (e.g., as a result of being accidentally pulled or jarred during maintenance work involving adjacent terminations or components). In general, instrument panel/cabinet wiring is bundled and secured to the panel support members so that any single termination would be exposed to only a fraction of the force that the bundle would experience. The staff considers the 0.004-ohm maximum conductor-to-termination resistance value acceptable. The voltage drops created by such resistances should have negligible impact on the performance of plant equipment.

The licensee applied the secureness verification criteria to a sample (34) of the compression lug terminations removed from the ICS cabinets after being identified as deviations during the visual inspections. All 34 terminations passed the secureness verification mechanical (8-pound) and electrical test criteria. The licensee believes this demonstrates conservatism in the visual inspection criteria, and believes that the secureness verification criteria can be used to augment the visual inspections.

The licensee expanded the scope of the Electrical Termination Inspection and Upgrade Program from the non-safety-related ICS/NNI cabinets to include visual inspections and secureness verification tests of terminations in the safety-related reactor protection system (RPS) cabinets and safety features actuation system (SFAS) cabinets, primary system control panels, the reactor ICS control console, and the process recording console. The expanded test scope resulted in the testing of an additional 8950 compression lug terminations. The licensee identified 9 failures which were subsequently replaced, and 1900 deviations that were either reworked or replaced to meet the test criteria. Of the 9 failures, 1 new failure mode was identified. One termination failure was caused by insufficient insertion of the assembled compression lug into the crimping tool. This placed the conductor insulation crimp too far forward on the lug barrel, causing pinching and shearing (although not complete severing) of the conductor strands. An additional type of deviation was also found that had not been identified during the visual inspections of terminations within the ICS/NNI cabinets: improper positioning of the lug relative to the crimping tool (i.e., improper crimp position).

While performing rework/replacement activities on the SFAS cabinets, two additional failure modes were identified in the area of internal terminations: (1) bare conductor protruding through the tongue end of the lug barrel with the conductor strands secured under the terminal board screw; when the screw was removed, the conductors slid out of the lugs and (2) conductor insulation extending through and visible at the tongue end of the barrel causing the barrel crimp to cover insulated conductor instead of the bare conductor wire strands. These failures prompted the licensee to visually reinspect internal terminations within the ICS, NNI, RPS, and SFAS cabinets. The licensee identified an additional 6 failures and 2100 deviations out of the approximately 9000 compression lug terminations reinspected. Again, the failed lugs were replaced, and the deviations were either reworked or replaced.

The licensee also discovered that during the installation of external compression lug terminations, some lugs were physically trimmed in order to fit better the terminal blocks supplied by the manufacturer. A total of 31 terminations were replaced because the trimmed lugs did not comply with the acceptance criteria specified by the vendor for the terminations. The licensee has developed procedures to preclude modifying lug terminations in the future.

In addition to compression lug terminations, the licensee also inspected solder terminations and wire wrap terminations within the ICS, NNI, RPS, and SFAS cabinets. The licensee stated that the inspection results showed a lack of consistent workmanship standards applied by the manufacturer during installation of both the solder and wire wrap terminations. Of the 23,400 solder terminations inspected by the licensee, 2 failures were identified, and 2500 deviations from the licensee's workmanship standards were identified. The types of deviations included:

- spattered flux
- insufficient or excessive solder
- grainy or porous connection
- improper tinning or wetting
- icicles or bridging
- damaged conductor insulation
- insufficient insulation clearance

Of the 8750 wire wrap terminations inspected by the licensee, 3 failures were identified, and 1130 deviations from the licensee's workmanship standards were identified. The types of deviations included:

- wire separation, consecutive coils not in contact
- wire coil overlays
- bent wire wrap pins
- broken or insufficient number of coils
- improper insulation clearance

The licensee has reworked solder and wire wrap termination deviations to comply with their workmanship standards.

During performance of the Electrical Termination Inspection and Upgrade Program, the licensee also performed general maintenance work on the cabinets/panels and components to correct other problems and deficiencies that were identified. These deficiencies included:

- component leads not covered with insulation
- terminal blocks with chipped or broken barriers
- terminal blocks not labeled
- drawing configuration discrepancies
- damaged printed circuit cards
- loose terminal board screws
- broken cabinet ventilation fans

Additional maintenance work performed included:

- cables rerouted and resupported
- conductor tie wrap supports added
- fuse panels cleaned and repaired
- cabinets cleaned and filters replaced
- modules cleaned and reworked

A total of 36 instrument panels/consoles/cabinets were included in the scope of the Electrical Termination Inspection and Upgrade Program. The licensee has reverified that all terminations within the program scope were inspected/tested. The program extended beyond the inspection of the ICS cabinets' internal compression lug terminations (such as the failure that contributed to initiation of the December 26, 1985 event) to include internal and external compression lug terminations within both safety-related and non-safety-related cabinets supplied by the ICS vendor. In addition, the inspection scope was expanded to include other terminations such as solder and wire wrap connections. Efforts were made to resolve other panel/cabinet deviations and deficiencies noted during the inspection process, and to perform general maintenance work to upgrade the overall condition of the enclosures and their components. Approximately half of all control room and computer room instrument panels/consoles/cabinets were included in the program. The licensee has stated that a program for the long-term inspection of other electrical plant panels has been initiated.

The licensee inspected 44,100 terminations (lugs, solder joints, and wire wraps) and identified 22 failures. The failure rate is approximately 1 in every 2000 terminations inspected, or 0.05%. Of the 22 failures, 12 were factory-installed "internal" compression lug terminations, 5 were licensee-installed "external" compression lug terminations, 3 were wire wrap terminations, and 2 were solder terminations. The licensee has concluded that the low failure rate demonstrates that no overall termination failure problem, and hence no significant safety hazard existed.

Of the 44,100 terminations inspected, approximately 7800 deviations from the licensee's inspection criteria were identified. Thus, a deviation was identified in approximately 1 out of every 6 terminations inspected, or roughly 17% of the terminations. The licensee has indicated that many of the deviations were reworked or replaced not because of unacceptable electrical connections or non-compliance with vendor specifications, but because the terminations did not conform to the licensee's more stringent criteria for workmanlike standards. The licensee stated that most of the termination deviations and deficiencies would have been identified either before the vendor delivered the terminations or when the terminations were delivered, if adequate acceptance and inspection criteria had been established.

Conclusions

The staff concludes that the Electrical Termination Inspection and Upgrade Program developed by the licensee was thorough and comprehensive with respect to the types and numbers of terminations inspected, and that the program was sufficient for determining the extent of potential problems concerning bad electrical connections within instrument cabinets/panels at Rancho Seco (similar to the bad connection within ICS cabinet 1 that was identified as a contributor to the root cause for the December 26, 1985 event). The staff further concludes that the licensee's criteria for identifying deviations during the termination

inspections were conservative and appropriate, and that the numerous termination replacements and reworks, and additional cabinet upgrades and maintenance activities have resulted in an increase in cabinet/panel quality and represent an overall improvement in plant safety. The staff concludes that the program was sufficient to ensure that concerns regarding bad electrical connections that were identified during investigation of the December 26, 1985 event will not exist within the safety-related RPS or SFAS cabinets, or within the non-safety-related ICS/NNI cabinets, at the time of plant restart.

The staff agrees with the licensee that the failure rate of instrument cabinet electrical terminations was sufficiently low to support the conclusion that no significant safety problem existed. However, the failures identified should not be dismissed as being insignificant. Failures of electrical connections such as occurred in ICS cabinet 1 before the December 26, 1985 event would represent undetectable failures if not identified during periodic surveillance testing. The characteristics of the bad electrical connection in ICS cabinet 1 were found to change with time. A similar bad connection in a safety-related system might not be detected during surveillance testing (i.e., would represent an undetectable failure), and its impact during a plant transient or accident could be significant, especially when considered in the presence of a postulated worst-case single failure, consistent with the plant licensing design basis. The number of failures identified, although small, in conjunction with the number of cabinet upgrades/maintenance activities required, highlights the importance of periodic cabinet inspections and good maintenance practices to ensure that the quality of the cabinets and their components is maintained. The licensee has stated that the development of maintenance criteria and procedures, and emphasis on high standards of workmanship will provide assurance of the future quality of electrical termination installation and maintenance. The staff concludes that the program will be effective in resolving concerns about bad electrical connections and in improving overall instrument panel/cabinet quality. The root cause of the event has been identified and measures have been taken to ensure against recurrence. This issue is resolved and is closed as a restart issue.

3.1.2.2 Loss of ICS/NNI System dc Power

ICS/NNI dc Power Distribution System

This section describes in detail the distribution of dc power within the ICS and NNI system. The role of ICS dc power in the December 26, 1985 event and modifications proposed by the licensee are also described, and the proposed modifications are evaluated.

ICS/NNI dc Power Distribution Before the December 26, 1985 Event

The ICS and the NNI system each consists primarily of (in addition to field-mounted equipment and control room indications and controls) several cabinets containing individual rows of rack-mounted modules. Each module serves a specific function (e.g., proportional amplifier, summer, integrator, control relay). The modules require nominal supply voltages of +24 V dc and -24 V dc, ±10%. The modules are not designed to ensure proper operation if the supply voltage strays outside of the ±10% band (i.e., less than ±21.6 V dc

or more than ±26.4 V dc). Testing has shown that at supply voltages only slightly below the specified minimum, some modules will malfunction and relays will begin to cycle on and off. If the dc supply voltage varies from ±24 V dc by more than ±10%, the performance of the ICS/NNI system becomes undefined and unanalyzed, and is considered unacceptable.

The NNI system at Rancho Seco consists of three subsystems: NNI-X, NNI-Y, and NNI-Z. Distribution of dc power within the ICS and NNI-X, and within the NNI-Y and NNI-Z is illustrated in Figures 3.18 and 3.19, respectively. These figures show the dc power systems as modified after the December 26, 1985 event. Although some design changes have been made (as discussed below), the basic distribution of power to ICS/NNI system dc loads has essentially remained unchanged from the time of the event. As discussed in SER Section 3.1.1.2, the ICS, NNI-X, and NNI-Y dc power supply systems each consist of two redundant pairs of ±24-V dc supplies. Each pair (one positive power supply and one negative supply) is energized by one of the two incoming 120-V ac feeders. Each pair of supplies feeds the positive and negative 24-V dc distribution buses through isolation diodes. The diodes act to separate the redundant pairs of supplies, and to provide "auctioneering" between the supplies (i.e., if the output voltage of one of the supplies is significantly higher than that of the other, the diode associated with the supply having the lower output voltage will be reverse biased, shutting off current flow through that diode, and the supply with the higher output voltage will provide power to the bus loads). If the output voltage of either supply should fall for any reason, the redundant supply is designed to assume the full load. Accordingly, the loss of either one of the incoming ac power feeds or one of the redundant pairs of dc power supplies should not have a direct affect on the dc-powered portion of the ICS/NNI system.

The NNI-Z subsystem consists of one pair of auctioneered -24-V dc supplies that provide power to relays used to select between redundant NNI-X and NNI-Y instrument channel (transmitter) inputs to control room indicators, annunciators, the computer, and the ICS. The relays are controlled by the operators from the control room using manual selector switches. The NNI-Z subsystem dc power supplies receive ac power from the NNI-Y subsystem.

The dc power system design includes overvoltage and undervoltage protection features to preclude system operation when the ±24-V dc supply voltage is outside of the specified ±10% band. Different methods are used for overvoltage and undervoltage protection, but in both cases, final protection is provided by a power supply monitor (PSM) module which is designed to transform a degraded voltage condition on either the positive or negative 24-V dc bus (a condition where the ICS/NNI system modules are subject to malfunctioning) into a complete loss of voltage condition for both the positive and negative 24-V dc buses (an easily detected condition where the module and plant response is more predictable, and from which better defined corrective actions can be initiated). If voltage on either the positive or negative 24-V dc bus is lost (e.g., because of multiple power supply failures or because of fault conditions within the dc power distribution system), but the other bus continues to supply its loads, operation of many system modules will become unbalanced, leading to potentially abnormal/erratic control system behavior and false control room indications (meters and recorders).

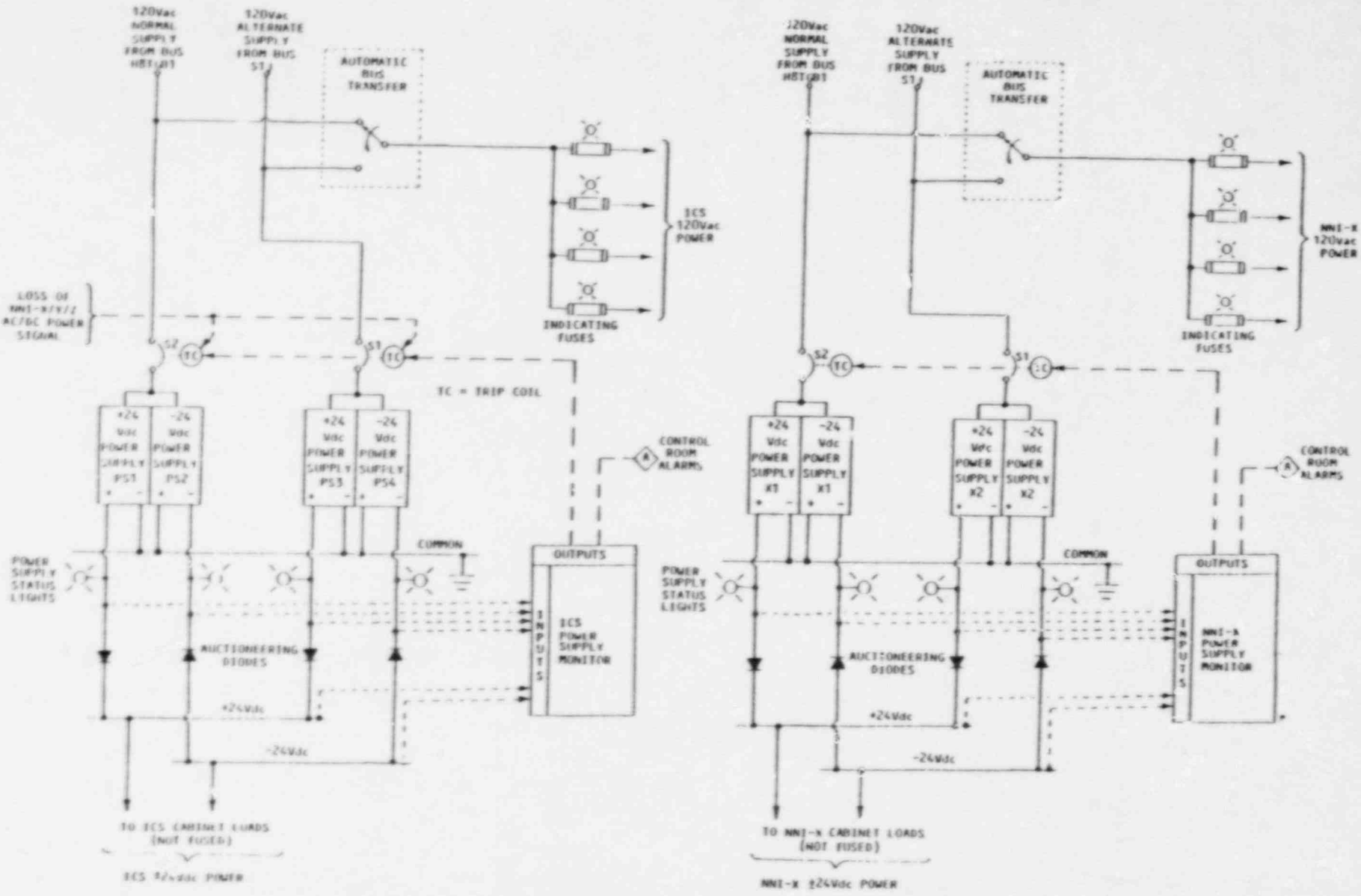


Figure 3.18 ICS and NNI-X dc power distribution

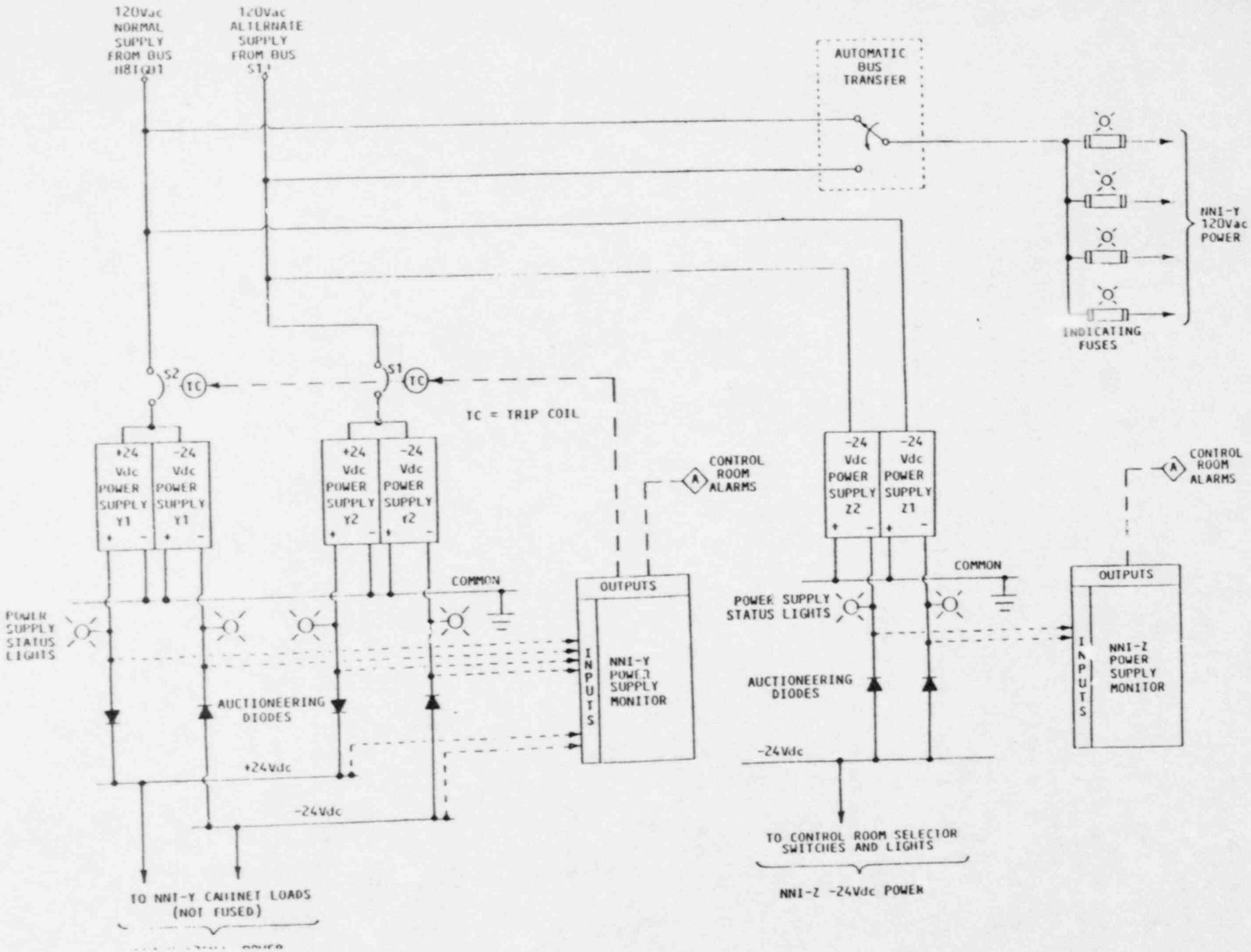


Figure 3.19 NNI-Y and NNI-Z dc power distribution

Overvoltage protection is provided within the ±24-V dc power supplies themselves. Each supply contains circuitry that automatically short-circuits its output terminals (causing an excessive overcurrent condition) whenever an overvoltage condition in excess of a predetermined setpoint value is detected. This circuit is referred to as a "crowbar" circuit. Overcurrent protection circuits internal to the power supply will turn the supply off upon sensing the excessive current caused by the crowbar circuit. The loss of voltage, or more accurately, an undervoltage condition of less than the setpoint value of 22.0-V dc, is then detected by the PSM, similar to an actual undervoltage condition. The PSM module is basically a set of undervoltage detection circuits and associated output relays mounted on a single, printed, circuit board. Upon sensing undervoltage, the PSM is designed to interrupt the ac power feeds to both pairs of ±24-V dc supplies (after a time delay of approximately 0.5 second) by automatically opening shunt trip switches S1 and S2.

A separate PSM module is provided for each of the ICS, NNI-X, and NNI-Y dc power systems. Each PSM includes six undervoltage detection circuits. Two undervoltage detection circuits per PSM are used to monitor the output voltages of the two associated positive 24-V dc power supplies, and similarly, two other undervoltage detection circuits monitor the two negative 24-V dc supplies. The remaining two undervoltage detection circuits per PSM are used to monitor the +24-V dc bus and the -24-V dc bus. Each undervoltage detection circuit operates one of four PSM output relays. One output relay deenergizes to actuate a control room alarm upon detecting an undervoltage condition at the output of either positive 24-V dc supply, and a second output relay similarly actuates an alarm upon detecting an undervoltage condition at the output of either negative 24-V dc supply. These alarms indicate the need to initiate maintenance because of the loss of dc power supply redundancy (i.e., the supply should be promptly restored to service to prevent a subsequent supply failure or fault condition from initiating a plant transient because a complete loss of ICS/NNI system dc power occurs).

The remaining two output relays per PSM are used to interrupt all incoming ac power feeds to the redundant pairs of dc power supplies by actuating shunt trip switches S1 and S2 upon detecting an undervoltage condition on the positive or negative 24-V dc buses. These output relays also actuated the same control room alarms to alert the operators to the loss of ICS/NNI system dc power condition. A PSM is also provided for the NNI-Z subsystem. This PSM does not perform any trip functions, but does provide alarms to the control room upon detecting an undervoltage condition on the NNI-Z -24-V dc bus.

Four separate control room alarms were provided at the time of the December 26, 1985 event, one alarm actuated by each of the ICS, NNI-X, NNI-Y, and NNI-Z PSMs. These alarms were labeled:

- ICS OR FAN POWER FAILURE
- NNI OR FAN-X POWER FAILURE
- NNI OR FAN-Y POWER FAILURE
- NNI Z POWER FAILURE

The ICS modules are located within five instrument cabinets just outside of the primary operating area of the control room. The ICS ±24-V dc buses are located inside cabinet 3. In general, power is distributed to individual ICS dc loads

via one of three main branch circuits. The first branch feeds ICS cabinets 1 and 2 (power to cabinet 2 loads is routed through cabinet 1); the second branch feeds cabinets 3 and 4 (cabinet 4 receives power in series with and downstream of cabinet 3); and the third branch feeds cabinet 5. However, not all ICS modules receive power in this manner (some control relay modules located in cabinet 3 get their 24-V dc power from cabinet 2, and some control relay modules located in cabinet 2 get their 24-V dc power from cabinet 3). The individual rows of modules within the cabinets are, in general, powered in parallel.

The PSM for the ICS ±24-V dc power distribution system was located in row 7 of cabinet 2. The actual voltage being monitored by the PSM was the voltage at the point at which the PSM received its power within the distribution system. Therefore, the PSM did not sense ±24-V dc bus voltage directly, but instead sensed bus voltage as supplied from the distribution system via upstream modules. It should be noted that in this configuration, the PSM will detect degraded voltage conditions within the distribution system caused by individual module failures upstream of the PSM sensing location, as well as detecting and providing protection against degraded voltages at the ±24-V dc buses. In the existing power distribution network within the five ICS cabinets, it is not possible to monitor the supply voltage to all of the modules with a single PSM. The ICS/NNI vendor (Babcock and Wilcox, B&W) has indicated that it was not a design objective to monitor the voltage to the modules of the system, but rather only to monitor the voltage on the ±24-V dc buses, which are the starting point of the dc power distribution system. A detailed discussion on the design and performance of the PSM, including the preferred PSM sensing locations, is provided in Section 3.1.2.8, "Power Monitor Design," of this report. The NNI-X and NNI-Y dc power distribution and PSM locations are not unlike those of the ICS.

The Role of ICS/NNI System dc Power During the Event

The December 26, 1985 event was initiated by the loss of dc power within the ICS. At the start of the event, several annunciators sounded in the control room, including the one labeled "ICS OR FAN POWER FAILURE." The control room operators realized immediately that a significant mismatch had occurred between reactor power and heat transfer to the steam generators, causing the pressure of the reactor coolant system to increase rapidly and initiating an automatic reactor trip. The operators realized approximately two minutes after the reactor trip that ICS dc power had been lost, but they did not initially understand the plant response to the power loss, nor did they realize that the PSM actuated shunt trip switches S1 and S2 had been tripped to the "OFF" position, thereby deenergizing the ICS dc power supplies.

In response to the loss of ICS dc power, several key ICS-controlled components went to the 50% demand positions, as designed. The turbine bypass valves went from the fully closed position to half open; the atmospheric dump valves went from the fully closed position to half open. These changes caused excessive steam to flow from the steam generators. The main feedwater and startup feedwater flow control valves went from almost fully open positions to half open, causing an inadequate flow of feedwater that resulted in the steam generators becoming ineffective at removing heat from the reactor coolant system. The loss of ICS dc power also resulted in the loss of remote manual

control for the above valves. Additionally, because the primary indicator for main feedwater flow failed to its mid-scale position, as designed, the reactor operators did not realize that main feedwater flow had been isolated because power had been lost to certain ICS control/interlock relays. Other control room indicators also failed to the mid-scale positions. The event is discussed in detail in NUREG-1195, "Loss of Integrated Control System Power and Overcooling Transient at Rancho Seco on December 26, 1985."

Twenty-six minutes after ICS dc power had been lost, the operators restored power by flipping the shunt trip switches (S1 and S2) back to the "ON" position. The restoration of ICS dc power restored remote manual control capability for ICS-controlled valves; however, the restoration of power also caused auto/manual control stations to automatically shift to the manual control mode and to generate output signals that demanded field equipment to go to the 100% positions, a result that the reactor operators did not expect. The effects of the response of the ICS to restoration of its dc power were not serious since many isolation valves had already been manually closed using local handwheels. Therefore, the reopening of the turbine bypass valves and atmospheric dump valves had no additional impact on the event. However, it was later realized that not only could the loss of ICS dc power cause a significant plant upset/transient, but that the response of plant equipment to the subsequent restoration of ICS dc power could significantly complicate recovery from the transient and increase the burden on the control room operators.

Modifications to the ICS/NNI System dc Power Distribution System

The licensee's investigation to determine the root cause for the loss of ICS dc power revealed that power was interrupted because of the automatic opening (tripping) of S1 and S2 by the PSM upon sensing an undervoltage condition associated with the +24-V dc bus. The root causes for the undervoltage condition have been attributed primarily to a bad wiring connection within the ICS dc power distribution system (the poor connection introduced a series resistance, and hence a voltage drop across the resistance, causing the PSM to sense a voltage less than the actual bus voltage), and secondarily to unstable operation of the PSM itself. The effects of the bad wiring connection and unstable PSM operation are discussed in Section 3.1.2.8, "Power Monitor Design," of this report.

The loss of a single dc power supply should have no effect on the ICS or plant operation. The December 26, 1985 event at Rancho Seco demonstrated that redundant dc power supplies can be lost. This fact (i.e., the total loss of ICS/NNI system dc power) had been demonstrated before the December 26, 1985 event, both at Rancho Seco and at other operating B&W reactors. The effects of a loss of ICS ±24-V dc power have included ICS-controlled equipment being driven from normal operating positions to the 50% demand position (e.g., control valves failing to half open), midscale failures of control room indications, and loss of remote manual control capability for ICS-controlled equipment. The effects of a loss of ±24-V dc NNI-X or NNI-Y power include numerous midscale failures of control room indicators (often the midscale failure positions are not noticeably different from the normal indicated values), and improper ICS response for the actual plant conditions because of the ICS controlling equipment positions are based on incorrect/failed input signals from the NNI system. Loss of ICS/NNI system power events at B&W reactors have caused plant

transients that challenge the operator's capability to mitigate the transient without resulting in overcooling or under-cooling of the primary system, and often involve both automatic and manual actuation of safety-related equipment to mitigate the transient. Testing and troubleshooting performed by the licensee after the December 26, 1985 event confirmed that the plant equipment performed as designed in response to the loss of ICS dc power. The testing also revealed that some of the control room indications and controls affected by the loss of ICS dc power behaved in a manner that had not been previously appreciated by the plant staff.

The licensee performed an analysis ("Deterministic Failure Consequence Analysis for NNI and ICS Power Supply Failure," dated July 26, 1986 and supplemented August 25, 1986) which addressed the likelihood and effects of losses of ac and dc power supplies and the associated plant responses. Past efforts to improve the reliability of the NNI system have focused on providing redundancy within the ICS and NNI system power distribution systems, thus making them less susceptible to single failures. A number of loss-of-ICS/NNI-system-power events, however, have occurred at B&W plants following modifications providing this redundancy. The licensee has, therefore, decided to focus corrective actions toward ensuring that the plant response to future ICS/NNI system power losses is such that the plant will assume a known safe condition without placing undue burden on the reactor operator. The deterministic failure consequence analysis (DFCA) supports, and the staff agrees with, this approach (i.e., preventing adverse ICS/NNI system-induced plant transients given a loss of power). The results of the DFCA showed that only a major change to the entire ICS control scheme would significantly alter the ICS failure modes. Therefore, the licensee has proposed a series of plant modifications to ensure that the plant response to ICS/NNI system dc power losses is known, predictable, and repeatable, so that the consequences of the power loss are less severe and can be mitigated through the use of specific procedures developed for the situation. The specific modifications and procedural changes to ensure that a known safe state will be achieved and maintained following ICS/NNI power losses are discussed in Sections 3.1.2.6, "Loss of Control Room Controls, Adequacy of Backup Instrumentation," and 3.1.2.10, "Operator Response Procedures," of this report. Specific changes to improve the reliability and performance of the ICS/NNI system dc power distribution system are discussed below.

The ICS and NNI-X ±24-V dc power supplies have been replaced with new, larger capacity supplies. The new supplies provide additional margin between the actual power supply load and the load capacity limit. A review of the NNI-Y and NNI-Z power supplies showed that sufficient margin existed, and that replacement was not necessary. Both the new and existing ±24-V dc power supplies are manufactured by the NJE Corporation. The power supply overcurrent and overvoltage protection setpoints (120% of rated current and 28.8 V dc, respectively) have been selected so that the power supplies are less susceptible to spurious trips, while still maintaining adequate protection.

The licensee has modified the ICS/NNI power distribution system so that an automatic trip of the ICS dc power supplies will occur (i.e., a forced loss of ICS dc power) anytime that NNI-X, NNI-Y, or NNI-Z dc power is lost, or any time that NNI-X or NNI-Y ac power is lost. Loss of ICS ac power will also result in the loss of ICS dc power. Therefore, whenever redundant power

supplies are lost within the ICS/NNI ac or dc distribution systems, a forced loss of ICS dc power condition results. The circuitry added to trip the ICS dc power supplies consists primarily of undervoltage relays used to sense the loss of NNI-X and NNI-Y 120-V ac power, and auxiliary relays used to sense the loss of NNI-X, NNI-Y, and NNI-Z ±24-V dc power. The relay contacts are then used to energize the existing trip coils for shunt trip switches S1 and S2 in the ac supply lines to the ICS ±24-V dc supplies. The same trip coils are actuated separately by the ICS PSM. NNI system 120-V ac power is sensed downstream of the automatic bus transfer (ABT) devices. Time delay on dropout (TDD) relays are provided to delay trip of the ICS dc power supplies for 1 second following loss of NNI system 120-V ac power to allow time for the automatic transfer to occur (the transfer should occur within 0.5 second). The added circuitry is shown in Figure 3.20. Both S1 and S2 must open to cause a complete loss of ICS dc power. The trip logic is arranged in a 2-out-of-2 configuration to minimize the probability of spurious losses of ICS dc power from a single failure. A status light has been mounted on the front of the NNI-X cabinet to indicate a half-trip condition such as could be caused by failures within the added circuitry. The light is on only when all relays are in the untripped/energized state (i.e., when all NNI system ac and dc power is available). Periodic observation of the indicating light will permit early detection of a half-trip condition.

The basis for tripping ICS dc power upon losses of NNI system power is that the ICS controls main feedwater flow, main steam header pressure (turbine pressure regulation), and reactor control rod movement (to make changes in reactor power level and maintain a constant reactor coolant average temperature, Tavg) based on more than 20 input signals it receives from the NNI system. Losses of NNI system ac or dc power can result in degraded/erroneous signal information being provided to the ICS, in turn causing undesirable ICS control actions for the actual plant conditions. The licensee has made modifications to ensure that the response of ICS-controlled equipment to a loss of ICS dc power are well defined and will not result in severe plant upsets. Therefore, instead of a number of potentially different transient scenarios with varying consequences (i.e., the effects of a loss of NNI-X ac power would differ from the effects of a loss of NNI-Y dc power, etc.), the effects will always be those associated with a loss of ICS dc power where the plant has been modified to ensure that a known safe condition is reached, and where the operators can respond to all ICS/NNI system power failures using a single procedure on which they have been trained. In general, a known safe state is ensured by causing an automatic trip of the main feedwater pumps upon loss of ICS dc power. This results in a reactor trip on high reactor coolant system pressure, and subsequent automatic initiation and control of auxiliary feedwater flow by the safety-related emergency feedwater initiation and control (EFIC) system to ensure adequate heat removal. In addition, the turbine bypass valves are designed to fail closed, as are the atmospheric dump valves (which have been removed from the ICS and are now controlled by the EFIC system) to prevent subsequent excessive steam flow from the steam generators and potential overcooling conditions. The EFIC system is discussed in detail in Section 3.1.3 of this report.

During initial plant startup, a one-time integrated loss of ICS/NNI system power test will be performed to verify: (1) that main feedwater pumps trip on loss of ICS dc power and (2) that the ICS ±24-V dc supplies will trip on loss of NNI system power as designed. Following this initial startup test, the

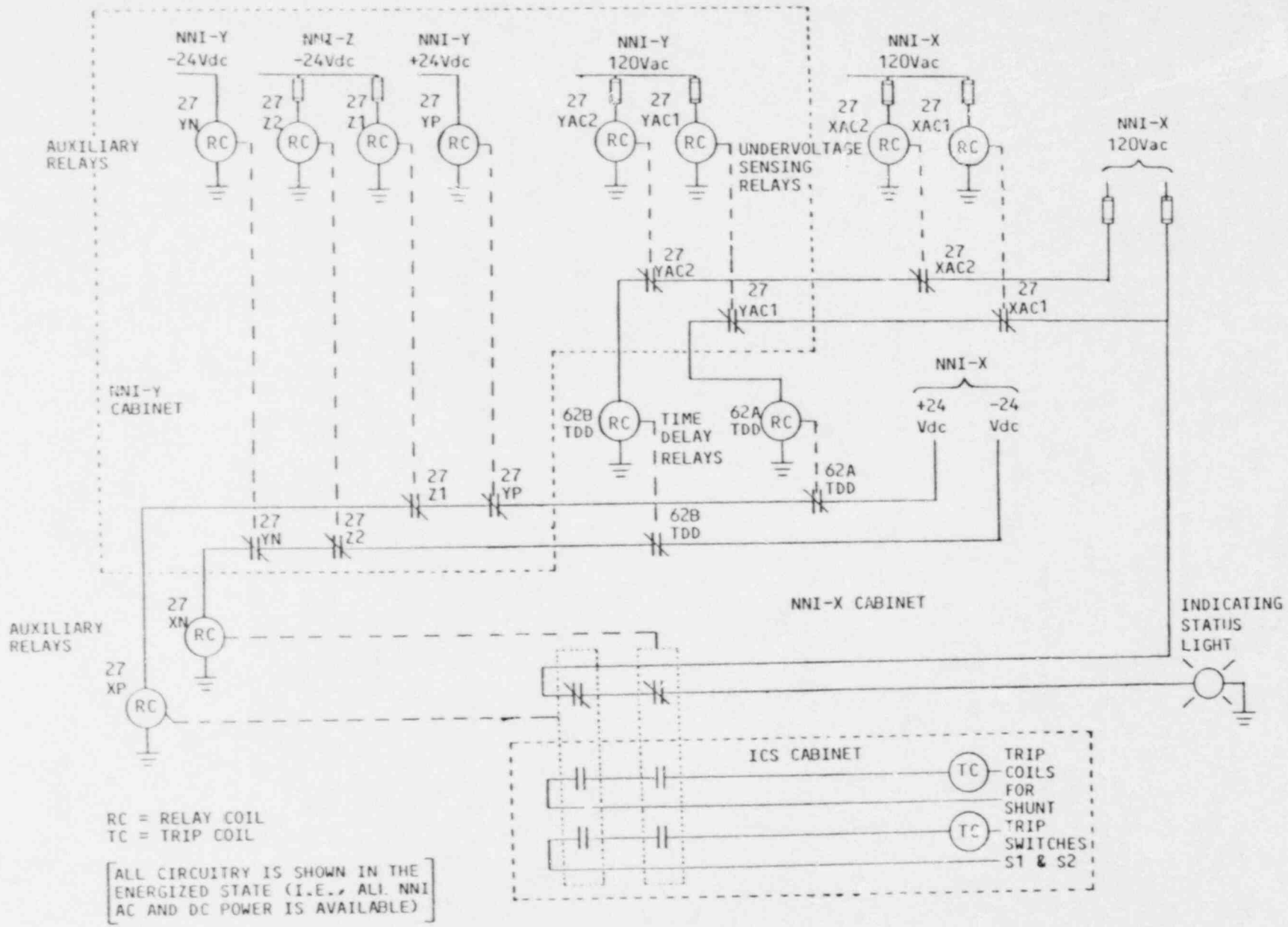


Figure 3.20 Automatic trip of ICS dc power on loss of NNI system ac or dc power

circuits will be functionally tested every refueling outage as part of the ICS and NNI system functional test programs. ICS/NNI system surveillance testing is discussed in Section 3.1.2.9 of this report, "ICS/NNI System Maintenance, Surveillance, and Testing."

The DFCA showed that loss of NNI system dc power can result in loss of both primary and secondary system controls, and loss of control room indications, making it difficult for the operator to act. Loss of NNI-X, NNI-Y, or NNI-Z dc power can result in loss of controls and/or indications for:

- pressurizer level and temperature
- reactor coolant pump seal flow and temperature
- letdown/makeup level, flow and temperature
- once-through steam generator level and pressure
- feedwater flow and temperature

Regarding loss of indications in the main control room, the licensee is taking the approach of essentially abandoning these indications if power is lost. The indicators are being labeled as to their dependency upon NNI system and ICS power, and will be ignored by the operators upon receipt of ICS/NNI system failure alarms. Also, considerable effort is being expended to ensure that backup instrumentation systems such as the safety parameter display system (SPDS) and postaccident monitoring instrumentation (installed in accordance with Regulatory Guide 1.97, Revision 2) will provide indications that are independent of, and therefore unaffected by, ICS/NNI system power losses. The failure of control room indications because of ICS/NNI system power losses, and the adequacy of backup indications are addressed in Section 3.1.2.6 of this report, "Loss of Control Room Controls, Adequacy of Backup Instrumentation."

The licensee has taken actions to improve the operator's ability to recognize the loss of ICS/NNI system dc power. The labeling of shunt trip switches S1 and S2 has been improved to make it more obvious when the switches are in the tripped position. Simple diagrams of the ICS power system have been posted on the door of the cabinet housing the ±24-V dc power supplies. Similar diagrams of the NNI power system were added to the cabinets housing the NNI system supplies after a loss of NNI system power event in 1978. In addition, indicator lights showing the energized/deenergized status of each of the ICS dc power supplies have been added to the outside of ICS cabinet 2. This will allow the operators to determine the status of the individual ICS dc power supplies without having to open the cabinet doors. The status lights will be operated by the output contacts of the portions of the PSM that monitors the individual power supplies. Therefore, these lights will, in effect, monitor not only the status of the power supplies but also the status of these portions of the PSM. Status lights for the NNI-X, NNI-Y, and NNI-Z dc power supplies were added in 1978.

In addition, the licensee has improved the control room annunciation of ICS/NNI system power losses to prevent misleading/confusing information being provided to the operators. The annunciation of losses of redundancy within the ICS ac and dc power distribution system is provided by system trouble alarms (i.e., "ICS TROUBLE" and "NNI TROUBLE"). The "NNI TROUBLE" alarm is shared by the NNI-X, NNI-Y, and NNI-Z subsystems. ICS/NNI system ±24-V dc power would still be available in this situation. The annunciation of losses of redundant

ICS/NNI system power supplies resulting in power failure is provided by system failure alarms (i.e., "ICS SYSTEM FAILURE," "NNI-X FAILURE," "NNI-Y FAILURE," and "NNI-Z FAILURE").

Another modification to the ICS/NNI system dc power distribution systems involves relocation of the input signals to the PSMs. The licensee has proposed to sense ±24-V dc bus voltage directly at the buses instead of indirectly at the PSM module location within the distribution system. The adequacy of the new PSM sensing location is evaluated in Section 3.1.2.8 of this report, "Power Supply Monitor Design."

In the first days after the December 26, 1985 event, tests were conducted in the control room to determine the affects of restoration of ICS dc power. The tests were repeated twice to confirm the results. Not all initial demand signals for key ICS-controlled valves went to 100% upon power restoration, as was thought to have occurred during the event. Not only did the auto/manual control stations reinitialize to different demand values, but some demand signals changed with time. Generally, the demand signals were either 0 or 100%. Some of the test results were inconsistent or unexplained. The demand for the turbine bypass valves went to 0, while the demand for the atmospheric dumps valves went to 100%. The demand for the train A flow control valve went to 100%, while the demand for the train B valve went to 0. The demand for the speed of both main feedwater pumps went initially to 100%, decreased to 50% over the next 31 seconds, and then decreased slightly more rapidly to 0 during the next 25 seconds.

After the December 26, 1985 event, the B&W Owners Group (BWOG) performed loss-and-restoration-of-ICS, ac and dc power tests at the Davis-Besse nuclear plant. The loss-of-ac-power tests showed that all the auto/manual stations reinitialized in the manual control mode with an initial demand signal determined by analogue memory modules associated with each of the stations. In each case, the initial demand signal selected was -10 V dc. For the main feedwater system flow control valves and startup valves, the -10-V dc value corresponds to 100% demand, or the fully open position. In the case of the turbine bypass valves, -10 V dc corresponds to 0 demand, or the fully closed position. These tests were repeated and demonstrated that the equipment response to restoration of power was repeatable and predictable. The loss-of-dc-power tests showed that all auto/manual stations went to the expected 50% demand signals, except for the turbine bypass valves and the atmospheric dump valves. At Davis-Besse, contacts from the PSM cause the turbine bypass valves to stay in the fully closed position, and power for the atmospheric dump valves came from a different source than ICS power so that these valves were unaffected. The restoration-of-dc-power tests showed that the auto/manual stations consistently reinitialized in the manual control mode with initial demand signals determined by the -10-V dc or +10-V dc value selected on the analogue memory modules associated with each auto/manual station.

Comparison of the test results at Davis-Besse with equipment performance at Rancho Seco during the December 26, 1985 event and subsequent testing revealed some important differences. The Davis-Besse design included features to avoid adverse effects from the loss and restoration of power to certain equipment (e.g., the turbine bypass valves and atmospheric dump valves), and the equipment response to restoration of power was predetermined and expected.

The licensee has modified the analogue memory modules in the Rancho Seco ICS to establish a known predictable state upon restoration of ICS power. In addition, the licensee has prepared a casualty procedure to address the restoration of ICS power. The licensee has elected to defer any attempt to restore ICS power until after the plant is stable in a safe-shutdown condition. Then, following procedures, the operators would take the necessary actions to prepare the system for power restoration. The basis for deferring restoration of power, as opposed to prompt restoration to regain remote manual control capability of ICS-controlled equipment, is that for some postulated failures such as bus faults, power could not be quickly restored. If the plant is assured of going to a known safe state upon loss of ICS dc power, then prompt restoration of power would not be necessary. However, for many situations, prompt restoration of power would appear to be highly desirable, especially if the plant is assured of remaining in a known safe state upon power restoration. The staff is currently evaluating the merits of prompt restoration of ICS/NNI system power as part of the review of the BWOG generic reassessment program for B&W plants (BAW-1919, "B&W Owners Group Safety and Performance Improvement Program").

Conclusion

The staff concludes that the licensee has taken appropriate actions to improve the performance of the ICS/NNI system dc power distribution system, and to significantly reduce the impact/consequences of loss of ICS/NNI system power events. Improvements to the dc power system include new larger capacity ±24-V dc power supplies for the ICS and NNI-X system, local indicating lights to provide for quick assessment of the status of the ICS ±24-V dc supplies, and more accurate (less confusing) annunciaton of loss of ICS/NNI system dc power events. A major improvement is the provision of circuitry to automatically trip all ICS dc power (i.e., cause a forced loss of ICS dc power condition) upon loss of NNI-X or NNI-Y ac power, or NNI-X, NNI-Y, or NNI-Z dc power. This modification, coupled with modifications to ensure that the equipment response to the loss and subsequent restoration of ICS dc power is known, predictable, and repeatable, is designed to ensure that the plant will assume a known safe state following ICS/NNI system power losses, and to allow the operators to maintain positive control of the plant through a common procedure developed specifically for the loss of ICS dc power. The staff concludes that the modified ICS/NNI system dc power distribution systems at Rancho Seco are acceptable for plant restart.

3.1.2.3 Loss of ICS/NNI System ac Power

ICS/NNI System ac Power Distribution System

This section describes in detail the design of the external ac power sources for the ICS and NNI system at Rancho Seco as they existed during the December 26, 1985 event, the role of this power in the event, modifications to the ICS/NNI system ac power distribution system proposed by the licensee following the event, and an evaluation of the adequacy of the modified design. The evaluation considers the performance of equipment affected upon loss of ac power, loss of all offsite power, and control room indications and alarms associated with the loss of ICS/NNI system ac power.

ICS/NNI System ac Power Distribution Before the Event

Distribution of ac power to the ICS and NNI system at the time of the December 26, 1985 event is illustrated in Figure 3.21. As discussed in SER Section 3.1.1.2, the Rancho Seco ICS/NNI system designs include provisions for two redundant ac input power feeds; a primary (normal) supply and a secondary (backup) supply. At the time of the event, the primary source of ac power for the ICS was one of the plant's four safety-related Class 1E 120-V ac vital instrumentation buses (bus S1C). The primary source for the NNI system was also one of the vital instrument buses (bus S1D). Vital instrument buses S1C and S1D are powered by Class 1E battery-backed inverters that convert dc power to highly regulated ac power suitable for instrumentation applications. During normal plant operations, the inverters are energized by their associated battery chargers. The battery chargers were, in turn, powered from 480-V ac sources that could be energized by the associated divisional emergency diesel generators (EDGs) upon a loss of offsite power. Power was provided to ICS bus S1C by the Division A EDG (GEA) via battery charger H4BC and inverter 1C, and power was provided to NNI system bus S1D by the Division B EDG (GEB) via battery charger H4BD and inverter 1D. During momentary interruptions of power from the battery charger, such as between losing offsite power and obtaining power from the EDG, the inverter would continue to operate by drawing power from the battery. The circuit breakers between the vital instrument buses and the ICS/NNI system served as the isolation devices between the safety-related portion and the non-safety-related portion of the design.

At the time of the December 26, 1985 event, the backup (alternate) power feeds for the ICS and for both NNI system sets of instrumentation (i.e., NNI-X and NNI-Y) were provided from one non-safety-related plant instrument bus (bus S1J). Bus S1J was also powered from a battery-backed inverter. Although bus S1J is a non-safety-related bus, the battery charger associated with the inverter could be powered from the Division A EDG upon loss of offsite power. It should be noted that a transfer switch was provided to allow the use of a standby source of ac power (non-Class 1E, non-battery-backed instrument bus S1F) to bus S1J when the normal battery-backed inverter was not available. At the time of the December 26, 1985 event, the power to the backup ICS/NNI system bus (S1J) originated from bus S1F.

In summary, at the time of the December 26, 1985 event, the primary sources of power for the ICS and NNI system were separate, safety-related, Class 1E 120-V ac vital instrument buses, and the backup power source was a non-safety-related, non-battery-backed, instrument bus.

The Role of ICS/NNI System ac Power During the Event

The primary sources of incoming ac power to the ICS and NNI system remained available throughout the December 26, 1985 event. This was determined by the observation that the automatic bus transfer (ABT) devices within the ICS and NNI system did not transfer to the backup power sources. The behavior of plant equipment also confirmed that ac power was not lost. Therefore, ac power to the ICS/NNI system was not a factor in the event.

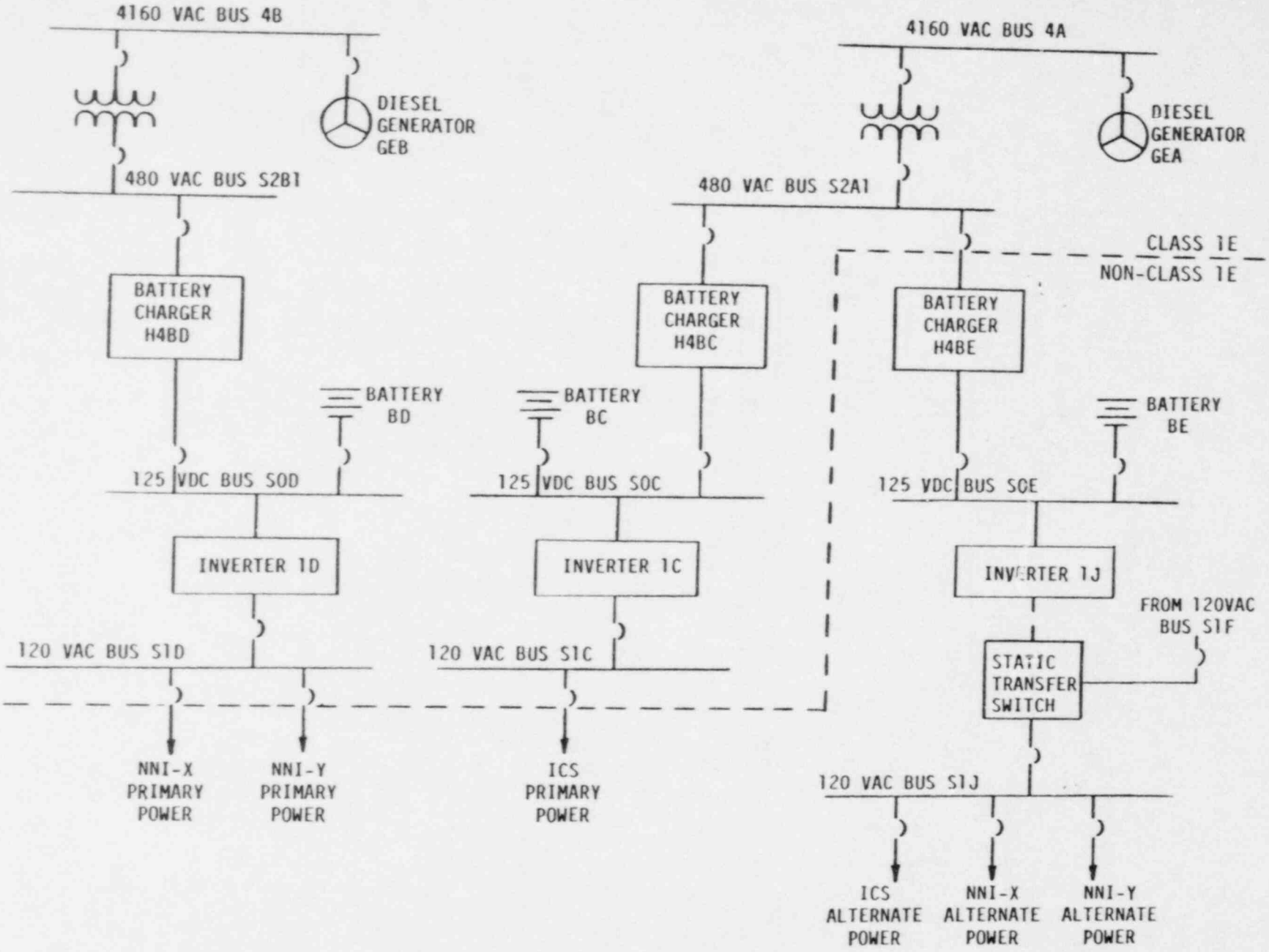


Figure 3.21 A simplified diagram of ac power distribution to the ICS and NNI system at Rancho Seco before the December 26, 1985 event

Modifications to the ICS/NNI System ac Power Distribution System

The licensee has instituted major plant modifications to improve the reliability and performance of the ac power distribution system at Rancho Seco. These modifications include installation of four new safety-related 120-V ac instrument buses, inverters, batteries, and battery chargers. The licensee has also installed two new non-safety-related instrument buses (S1GA-1 and S1GB-1), complete with new inverters, batteries, and battery chargers. The configuration for the primary and secondary ac power feeds to the ICS and NNI system in the modified design is shown in Figure 3.22. The primary 120-V ac power source for both the ICS and all non-nuclear instrumentation will now be instrument panel H8TGB1 which receives power from instrument bus S1GB-1. The backup power source for the ICS and NNI system will continue to be instrument bus S1J (bus S1J is connected in parallel with bus S1GA-1, and is backed by a new inverter and battery charger). All six battery chargers (four safety-related and two non-safety-related) will receive emergency power from two new large EDGs. The new EDGs are discussed in Section 4.7 of the Rancho Seco Restart SER. The battery chargers associated with the non-safety-related instrument buses also serve as the isolation devices to separate the Class 1E portion of the electrical distribution system from the non-Class 1E portion. Each of the new inverter assemblies includes a static transfer switch at the output, which provides for automatic transfer to a regulating transformer as an additional backup power source.

It should be noted that the licensee has been asked to evaluate the effects of loss of power to each safety-related and non-safety-related bus providing power to instrumentation and/or control systems, and to determine whether a safe shutdown condition can be readily achieved through the use of the remaining instruments and controls, as governed by plant operating procedures, following the power loss. The results of the licensee's evaluation are discussed in Section 3.1.2.11 of this report, "ICS/NNI System Interactions With Safety-Related Equipment."

If the single source of primary 120-V ac power to the ICS and NNI system were lost, the system design provides the capability to automatically transfer ICS and NNI system loads to the secondary (alternate) 120-V ac power source. If the alternate source and the transfer devices to the alternate source have been properly maintained, power from these sources will likely be available. Periodic maintenance and surveillance of the ICS/NNI system power distribution system is discussed in Section 3.1.2.9 of this report, "ICS/NNI System Maintenance, Surveillance, and Testing."

The control room alarms related to ICS/NNI system ac power failures have been modified to provide the operators with more accurate, non-confusing information. A new annunciator point, "ICS TROUBLE," has been provided in the control room, and will alarm the following conditions:

(1) any fuse blown in the ICS
(2) any cabinet fan failure in the ICS
(3) any dc power supply failure in the ICS

If the primary ac power source to the ICS should fail, and the automatic bus transfers to the alternate ac source, two control room annunciators will alarm:

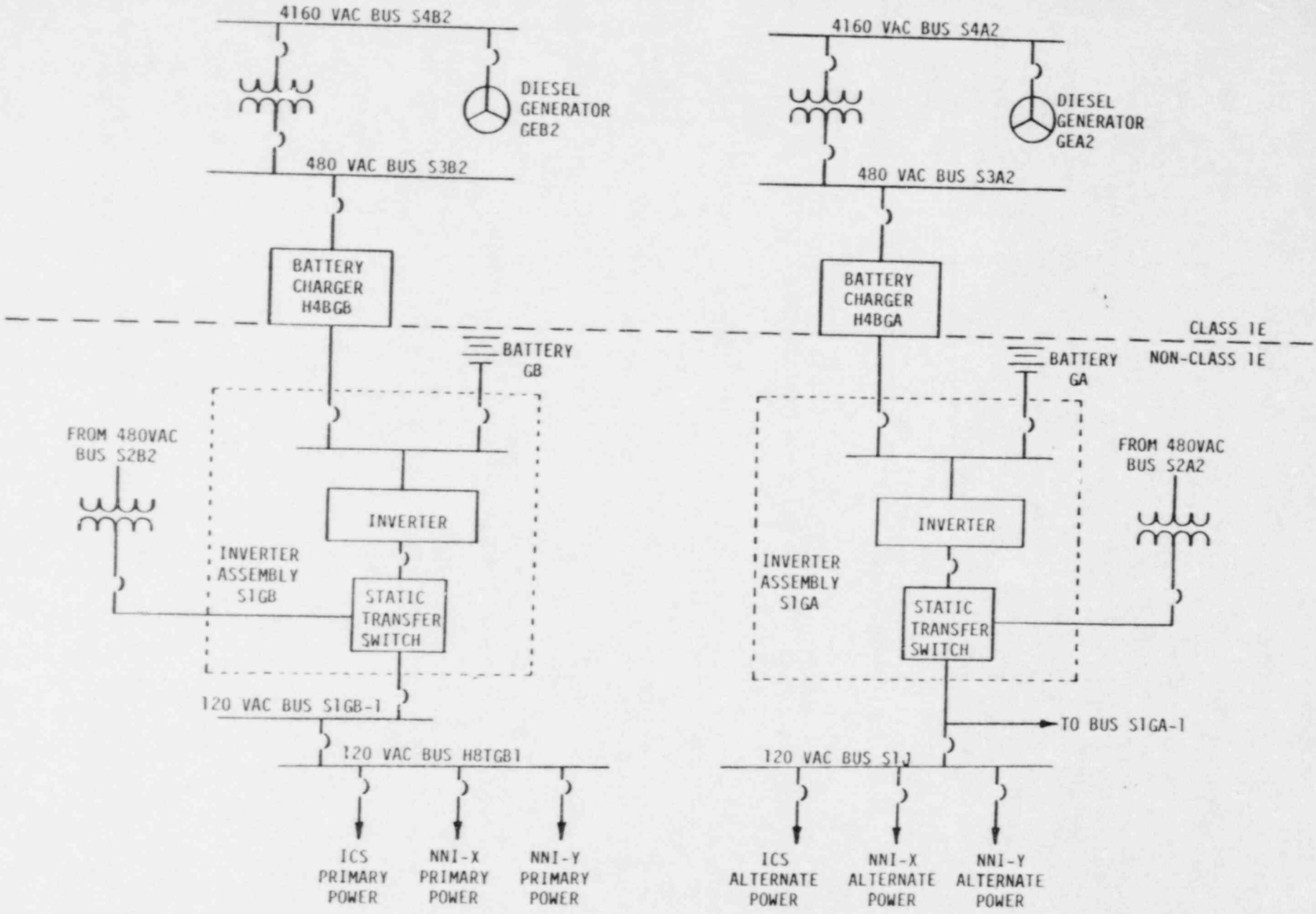


Figure 3.22 Current design of ac power distribution to the ICS and NNI system at Rancho Seco following modifications

"ICS TROUBLE" (due to the bus failure) and "ICS OR NNI 120 VOLT POWER TRANSFER" (due to operation of the ABT device). If the alternate/backup ac power source to the ICS should fail, two control room annunciators will alarm: "ICS TROUBLE" and "NON-VITAL POWER BUS 1E/1F/1J TROUBLE." Similar annunciator points have been provided for the NNI system. Upon receipt of one of these alarms, someone from the plant staff would be sent to the ICS/NNI system instrument cabinets and/or local equipment/switchgear rooms to determine the specific condition that activated the alarm and to initiate appropriate corrective action.

A new "ICS SYSTEM FAILURE" annunciator point has also been added. If both the primary and alternate sources of ICS ac power were lost (this would also cause the loss of ICS dc power), the "ICS SYSTEM FAILURE" alarm would actuate in the control room. "NNI-X FAILURE" and "NNI-Y FAILURE" alarms are similarly provided. The control room alarms provided on loss of ICS/NNI dc power are discussed in Section 3.1.2.2 of this report, "Loss of ICS/NNI System dc Power."

The staff considers the new ICS/NNI system loss-of-ac-power annunciator arrangement, which clearly indicates system level trouble (i.e., the system is operable although a degraded condition exists) versus system level failure (i.e., the system is not operable), an improvement over the previous design in which specific equipment status conditions were annunciated. The three separate battery-backed buses providing normal ICS/NNI system power, alternate ICS/NNI system power, and power to the control room annunciators, are normally powered from three separate battery chargers, that are in turn powered from three separate 480-V ac load centers. Therefore, a single bus failure cannot cause an ICS/NNI system loss of power and loss of control room annunciation of the loss of power. The effectiveness of ICS/NNI system loss of power annunciation also depends on the adequacy of the plant annunciator response procedures and training of the operators. The annunciator response procedures are discussed in Section 3.1.2.10 of this report, "Operator Response Procedures."

If all sources of ac power to the ICS were lost (causing the loss of ac power to ICS field loads, control interlock relays, and to the ICS dc power supply system), a plant transient involving reactor trip and actuation of the auxiliary feedwater system would result because of the direct effect on ICS-controlled components. If all sources of ac power to the NNI-X or NNI-Y were lost, a significant number of control room indications would become inoperable, including safety features actuation system (SFAS) related instrumentation such as high-pressure injection (HPI) flows, core flood tank levels and pressure, decay heat system flows and temperatures, and nuclear cooling water flows. In addition, some SFAS annunciators are either failed or defeated. The net result is that the control room reactor operator's ability to verify specific safeguards actions is diminished. The loss of all NNI-X or NNI-Y ac power will also cause the loss of ICS dc power as discussed in Sections 3.1.2.2 ("Loss of ICS/NNI System dc Power") and 3.1.2.6 ("Loss of Control Room Controls, Adequacy of Backup Instrumentation") of this report. The overall plant response to ICS/NNI power failures is addressed in Sections 3.1.2.5 (ICS/NNI System Failure Modes and Effects Analysis") and 3.1.2.6.

Because of the consequences of a complete loss of ICS, NNI-X, or NNI-Y ac power, it is desirable to minimize the length of time for which either the normal or alternate source is unavailable. Plant operation for long periods of time with only a single ICS/NN system ac power source available increases the probability

for a single failure to cause a complete loss of ac power and an unwanted plant transient. The licensee has indicated that an inoperable ac supply to the ICS/NNI system will be promptly restored to an operable status to better ensure plant availability.

The licensee performed an analysis ("Deterministic Failure Consequence Analysis for NNI and ICS Power Supply Failure") that considered the failure of an ABT device to transfer the source of ICS/NNI system ac power from the primary (normal) source to the backup (alternate) power source upon failure of the normal source. An ABT failure of this nature would result in a complete loss of ICS/NNI system ac power. The licensee does not plan to modify/upgrade the ABT devices because operating experience at Rancho Seco has shown that the devices are reliable. It is noted that during the March 19, 1984 loss of NNI system power event at Rancho Seco, an ABT transfer was interrupted because of an improper setpoint value. The licensee performs periodic (yearly) surveillance of the ABT devices (including calibration of the transfer voltage setpoint value) to verify their operability, and to ensure that the reliability of these devices is maintained.

Since the redundant sources of ac power to the ICS/NNI system are ultimately powered from the redundant Class 1E, EDG-backed, safety-related emergency buses, a loss of offsite power should not affect the operation of the ICS/NNI system.

Conclusion

The licensee has taken significant actions to improve the design reliability of the ac power sources for the ICS and NNI system, including improved control room annunciation of ICS/NNI system power losses. The ac power feeds to the ICS/NNI system are redundant and independent so that any single 120-V ac bus failure (or the failure of any connected upstream bus) should not adversely affect the ICS/NNI system. During the December 26, 1985 event, ICS/NNI system ac power remained available and was not a factor. The staff concludes that the ICS/NNI system ac power distribution system is acceptable for plant restart.

3.1.2.4 Loss of Instrument Air to ICS/NNI System Components

Instrument Air System

Following the December 26, 1985 event at Rancho Seco involving a partial loss of ICS power and a subsequent overcooling transient, the licensee performed an in-depth review and evaluation of other systems critical to secondary-side heat removal. One of the selected systems was the instrument air system (IAS).

Over the past year, the IAS at Rancho Seco has been evaluated by the licensee and by the Babcock and Wilcox Owners Group (BWOG). The evaluation by the licensee included an analysis, "Deterministic Failure Consequence Analysis" for NNI and ICS Power Supply Failure" (DFCA) of the IAS; in that document, the failure of each IAS component and the postulated total loss of IAS pressure was analyzed to determine the effect on plant operation at power. The analysts concluded that a loss of instrument air could lead to a significant plant transient with consequences more severe than the December 26, 1985 event. The BWOG stated in BAW-1919, "B&W Owners Group Safety and Performance Improvement Program," that

the potential effects of IAS failures are similar in extent and character to failures such as the loss of ICS power.

The licensee has identified a series of design modifications and procedural changes to improve IAS reliability and performance. The modifications include a backup diesel-driven air compressor and dryer package which is independent of site support systems (e.g., cooling water, power). Independent compressed gas bottle supplies will also be provided for critical plant instrument air-operated components (e.g., auxiliary feedwater flow control valves). The modifications will improve the plant response to either a sudden or gradual loss of instrument air pressure, and will be implemented before plant restart.

The evaluation that follows addresses the potential safety implications associated with the IAS, design modifications implemented before plant restart, the effects of a complete loss of instrument air, partial IAS losses which could affect a group of components, and restoration of instrument air. The staff concludes that the modified Rancho Seco IAS design and revised procedures should provide for a reliable source of air to pneumatic instruments and controlled components when required for achieving and maintaining safe shutdown conditions.

Background

The December 26, 1985 event raised concerns that the failure of a non-safety-related control system, the integrated control system (ICS), subjected the plant to an undesirable overcooling transient. NUREG-1195, "Loss of Integrated Control System Power and Overcooling Transient at Rancho Seco on December 26, 1985," concluded that the fundamental causes for the transient were design weaknesses and vulnerabilities in the ICS and equipment controlled by the ICS. A characteristic of the ICS that contributed to the severity of the transient is that it is involved in the operation/control of a large number of plant systems (e.g., feedwater control, rod control, turbine bypass valve control), and therefore, when the ICS fails, the effects are widespread throughout the plant. In addition, the non-safety-related ICS did not receive the periodic maintenance or surveillance that was given to or required for other (safety-related) systems to ensure their operability, even though the consequences of ICS failures can be more severe.

Similarly, the IAS is a non-safety-related system that is also involved in the operation/control of a large number of plant systems (e.g., feedwater control, reactor coolant system letdown and makeup flow control, component and plant cooling water flow control, turbine bypass valve control). The staff raised the concern that the effects of IAS failures could also be widespread throughout the plant and could lead to complicated/severe plant transients. Therefore, the staff requested that the licensee address the overall reliability of the Rancho Seco IAS, and specifically address the following items:

- The individual component response, including ICS and non-nuclear instrumentation (NNI) system components, to the loss of instrument air, and the potential effect of such responses on plant operation. The combined effects of multiple component failures that result from a complete loss of instrument air and partial losses of instrument air that could affect a group of components should be considered.

- The individual component response to the restoration of instrument air subsequent to IAS failures, and the potential multiple effects of restoration on the capability to achieve and maintain stable plant conditions.

- The potential for a loss of instrument air as a result of losing offsite power.

- The adequacy of control room indication/annunciation of loss of instrument air and IAS trouble.

- The adequacy of IAS maintenance, surveillance, and testing. Gradual loss of air pressure and sudden/instantaneous loss of air pressure should be tested and the proper system response should be verified as recommended in Regulatory Guide 1.68.3, "Preoperational Testing of Instrument Air Systems."

The IAS supplies pressurized air used to operate components that perform functions important to safety. Regulatory Guide 1.68.3 states that testing should be performed following major modifications or repairs to the IAS to verify that the system will respond appropriately to both normal operation of the plant and upset, faulted, or emergency conditions with considerations being given to:

- The complete and sudden loss of pressure resulting from such postulated events as inadvertent valve operation in the supply system, severance of a system pipe, loss of offsite electric power, loss of dc power, and component malfunction.

- The partial or gradual loss of system pressure to the entire distribution system or portions thereof resulting from such events.

- The increases in pressure that result from component malfunction or failure.

System Description

The Rancho Seco instrument air system (IAS) and service air system (SAS) are collectively referred to as the plant air system. The plant air system is designed to supply compressed air for pneumatic instrumentation and controls, and for general service air needs during all phases of plant operation. The Rancho Seco Updated Safety Analysis Report states in Section 9.10 that the plant air system serves no safety-related functions. However, a large number of air-operated valves essential to safe plant operation are provided air from portions of the plant air system.

Three, 275-SCFM capacity, nonlubricated reciprocal compressors with after-coolers supply the system with moisture-free, oil-free air at a nominal 100 psig via individual air receivers. The operational lineup assigns one compressor for continual service and a second compressor is set to load and unload with demand changes. The third compressor is maintained in an auto-start standby mode.

The plant air system separates downstream of the air receivers to form the IAS and the SAS. The distribution system for the IAS employs both loop and single line header designs. The turbine plant IAS distribution uses a loop layout and has local manually operated isolation valves located in the corners of the turbine building. The remaining headers are single line design. The SAS employs only single line runs.

The plant air system provides compressed air for operating valves, instruments, and controllers throughout the plant. Equipment, systems, and plant areas utilizing compressed air include the following:

Primary Systems
- component cooling water
- control rod drive cooling water
- hydrogen gas
- nitrogen gas
- nuclear raw water
- purification and letdown distribution
- radwaste
- reactor coolant drain
- reactor coolant system
- reactor sample
- seal injection and makeup
- waste gas

Secondary Systems
- auxiliary steam
- extraction steam
- feedwater
- auxiliary feedwater system
- gland steam and condensate
- heater, drain, and vents
- high-pressure turbine
- main circulating water
- main condenser and makeup
- main steam
- plant cooling water
- turbine plant cooling water
- turbine plant sampling

Auxiliary Systems
- demineralized water
- drainage and sewerage
- heating, ventilation, and air conditioning
- secondary chemical addition
- service water

The primary function of the IAS is to provide a continuous supply of dry, oil-free air to act as the motive force for all vital pneumatic valve actuators, instruments, and controls (e.g., safety-related diaphragm or cylinder-actuated valves and safety-related electric-pneumatic converters). Components unique to the IAS are (1) dual tower desiccant-type air dryers designed to maintain a dewpoint of -40°F at 100 psig (the main dryer is rated for 900 SCFM and the standby dryer is rated for 337 SCFM); (2) particulate air filters with filtering capabilities to 5 microns (three 200-SCFM units are used in parallel and simultaneously); and (3) a new dedicated backup diesel-driven air compressor

(DDAC) to improve system reliability in the event of a loss of offsite power or failure of the existing electric-motor-driven compressors.

The DDAC system consists of the compressor and its diesel engine, an aftercooler, air receiver, and a filter/dryer package. The DDAC can supply air to both the IAS and the SAS. The DDAC will automatically start if IAS pressure decreases to 85 psig, or upon loss of 120 V ac to the compressor skid. Engine starting power is provided by a 12-V battery, with 120-V ac power provided to a battery charger and engine block heaters. The backup air supply is isolated from the upstream IAS filters by a check valve.

The IAS supplies air for the ICS-controlled main feedwater (MFW) and startup feedwater (SUFW) control valves. To ensure that the MFW and SUFW valves can be closed and will remain closed if required by the emergency feedwater initiation and control (EFIC) system (the EFIC system is discussed in Section 3.1.3 of this report), a new 2-hour, seismic Class 1, backup supply of bottled air has been provided. The 2-hour time is based on engineering judgment and is considered sufficient to allow the operators to achieve a stable plant condition. The backup air supply is designed to conform to the criteria provided in ANSI/ANS Standard 59.3, "Safety Criteria for Control Air Systems." Two sets of high-pressure bottles and reducing stations have been provided. One set supplies air to MFW, SUFW, and EFIC system-controlled auxiliary feedwater (AFW) valves associated with once-through steam generator (OTSG) A; and the second set supplies air to MFW, SUFW, and EFIC system-controlled AFW valves associated with OTSG B. Each set uses high-pressure air bottles headered through a pressure reduction valve to supply air at a pressure of approximately 85 psig. Since the IAS supply pressure is approximately 100 psig, the backup air supply will only function if the IAS pressure decreases below 85 psig. Check valves are provided in the normal instrument air supply line to prevent flow from the backup supply into the normal supply following a loss of air, and to isolate a depressurized branch of the IAS.

The IAS also supplies the turbine bypass valves (TBVs). A backup supply of air is provided by an independent set of high-pressure bottles dedicated to the TBVs. The TBV backup air is classified as non-safety-related since the TBVs are not required to bring the plant to a safe condition for a loss-of-air event. The atmospheric dump valves (ADVs) controlled by the safety-related EFIC system are available to the operators for secondary-side pressure control. The ADVs are independent of the ICS, and have been provided with a redundant Class 1 safety-related backup bottled air supply.

The high-pressure (2400 psig) backup air bottles feed the valves via pressure regulators. The regulators incorporate 175-psig rupture discs, and a downstream relief valve in the piping to the valves is set at 120 psig. Local pressure indicators are provided for the bottle pressure and the header pressure to the valves supplied from each backup air station. The control valves that are provided with backup air bottles are:

- auxiliary feedwater control valves (Class 1)
- main and startup feedwater control valves (Class 1)
- atmospheric dump valves (Class 1)*

*The ADVs have a second backup system of air bottles as per Appendix R requirements.

- turbine bypass valves (Class 2)
- component cooling water reactor building isolation valves (Class 1)

The high-pressure backup air bottles are grouped with either three or six bottles per group, except for the component cooling water valves which are supplied by a single bottle. Each bottle group is chained for security, and can be removed for servicing as a pack. The bottles are actually sized to provide a 3-hour supply of backup air, although credit is only taken for 2 hours.

The speed changer valves for the main feedwater pump turbines also operate with instrument air. A backup air supply is not provided for these valves. The MFW pumps will trip upon loss of instrument air or ICS power.

Air-operated valves that are controlled by the NNI system through electric/pneumatic (E/P) converters are the letdown orifice bypass valve, pressurizer level makeup valve, and seal injection flow control valve. The normal air supply for the control and actuation of these valves comes from the IAS. The letdown orifice bypass valve and pressurizer level makeup valve fail in the closed position upon loss of instrument air. The seal injection flow control valve fails in the open position upon loss of instrument air. These failure modes are considered the "fail-safe" positions of the valves and have the least effect on plant operation.

The nitrogen gas system (NGS) provides a cross-tie to the IAS as a backup supply of compressed gas to support the functions of the IAS in an emergency situation. The cross-tie requires a manual lineup of valves to place the nitrogen supply in service. The high-pressure nitrogen header pressure is reduced at the cross-tie, to conform to the IAS pressure rating.

Service Air System

The primary functions of the SAS are to provide clean air to local hose stations throughout the plant, and for use in fluffing and transferring of ion exchanger resin beds. The SAS is also used for the remainder of the plant's air needs (e.g., non-safety-related equipment, routine maintenance activities, pneumatic tools, breathing air).

A single line is used to supply air from the SAS to the IAS. A "priority valve" provides automatic isolation of the SAS upon detection of low header pressure, directing all air flow to the IAS. The priority valve actuates at approximately 30 psi below the normal header pressure of 100 psig.

Discussion

The staff has performed several studies of instrument air systems and has reviewed operating experience related to air system problems and failures. Areas of concern related to instrument air systems include: (1) air system contamination with oil, water, desiccant, and rust or other corrosion products which could lead to potential common mode failure of multiple components, (2) inadequate testing of the IAS and air-operated/controlled equipment (safety-related equipment failures have occurred when non-safety-related IAS control air pressure decreased slowly rather than rapidly as would occur following an

air line rupture), and (3) excessive leakage within the seismically qualified portions of air systems (specifically check valves and relief valves).

In March 1987, the staff completed report AEOD/C701, "Case Study Report on Air Systems Problems at U.S. Light Water Reactors." The report presents aspects of air systems degradations and plant responses to air systems losses which are not addressed in previous studies. It also highlights more than two dozen events in which, contrary to licensing assumptions, a safety-related system failed as a result of an air system degradation or failure. Operating events involving the loss or degradation of air systems were judged to be safety significant because they may lead, under different circumstances, to potentially serious events and conditions which have not been analyzed in the Final Safety Analysis Reports (FSARs). The report presents five recommendations which, if implemented, would reduce reactor accident risks by reducing the likelihood for common mode failure of safety systems and by enhancing plant recovery from anticipated and unanticipated transients. The recommendations in the study address: (1) ensuring that air system quality meets the requirements specified by the manufacturers of the plants' air-operated equipment; (2) ensuring adequate operator response by formulating and implementing anticipated transient and system recovery procedures for loss-of-air events; (3) improving training to ensure that plant operations and maintenance personnel are sensitized to the importance of air systems and the vulnerability of safety-related equipment served by the air systems to common mode failures; (4) confirming the adequacy and reliability of safety-related backup accumulators; and (5) verifying equipment response to gradual losses of air to ensure that such losses do not result in events that fall outside FSAR analyses.

The licensee developed a Systems Review and Test Program (SRTP) to upgrade plant systems by identifying problems, correcting the identified deficiencies and testing the systems to verify proper operation. The IAS was one of the systems selected for detailed review. The licensee performed a deterministic failure consequence analysis (DFCA) for the Rancho Seco IAS. This analysis involved "failing" individual IAS components from the IAS piping and instrumentation diagrams (P&IDs), and analyzing the effect upon the IAS and the plant. All IAS components were addressed by the DFCA. Next, the entire IAS was "failed" and the effects upon the plant were analyzed.

The DFCA is a technique to determine the consequences of failures of systems and equipment at power operation and the impact on post-trip response capability, and to evaluate related procedural guidance provided to the operators. The intent of the analysis is to identify areas in which failures of plant systems or procedural inadequacies could potentially result in unnecessary reactor trips, unsatisfactory post-trip response, undue challenges to the operators, or unnecessary challenges to the safety systems. The analysis consisted of the following:

- identification of all IAS-supplied devices and their failure modes
- a component level comparison between the configuration existing in the plant and the associated drawings and procedures (with corrections and omissions noted)
- an evaluation of response scenarios to a total loss of IAS accident

- recommendations for modifications of the IAS equipment, documentation, procedures, and training

The DFCA initiating transient was a complete depressurization of the IAS. The immediate plant response was an automatic reactor trip on high reactor coolant system pressure. The loss of component cooling water to reactor building components would require a manual trip of the reactor coolant pumps. As a result of the loss of main feedwater, the AFW system would automatically start and operate at full flow because of the failed-open AFW control valves. The ADVs and TBVs fail closed, resulting in the opening of safety valves. The safety valves subsequently were assumed to fail open resulting in a rapid cooldown of the reactor coolant system (RCS). At an RCS temperature of 525°F, the analysis considers two possibilities: no operator action and correct operator action. Assuming no operator action, the RCS cooldown is assumed to continue resulting in a drained pressurizer, loss of natural circulation, and repressurization of the RCS (pressurized thermal shock conditions would likely occur). The analysis also notes that the steam generators would be overfilled by AFW, potentially resulting in water hammer and possible damage to steam lines. Assuming the operator takes proper action at 525°F, both AFW pumps would be manually tripped. The loss of secondary cooling would require initiation of "feed and bleed" cooling.

The analysis further considers the ideal case of correct operator responses performed by an average crew of 13 operators. In this scenario, it is concluded that the functions vital to establishing an RCS stable shutdown could be controlled. However, these actions were considered difficult even for the most experienced crews.

The DFCA committee concluded that the then-current IAS design in combination with the then-existing procedures and training was inadequate to support reliable and safe plant operation. Although the assumptions made in the analysis are considered conservative, the basic conclusion that the IAS and associated procedures and training should be modified are justified by the analysis results.

The DFCA committee concluded that IAS reliability must be improved for safer plant operation. The more significant DFCA reliability improvement recommendations for the IAS include equipment modifications, revised casualty procedures for loss of instrument air and improved operator training for dealing with a loss of instrument air transient. Specific modifications to the Rancho Seco IAS design and procedures implemented before restart include the following:

- Installation of a diesel-driven air compressor (hard piped into the existing system) with auto start capabilities.

- The actuators for the AFW control valves are spring loaded to fail open on a loss of IAS pressure. The fail-open mode could result in excessive AFW flow and rapid cooldown following a plant trip, similar to the December 26, 1985 transient. However, seismic Class 1, 2-hour rated backup air supplies have been provided for the AFW control valves to permit closure of the valves from the control room following a loss of instrument air.

- MFW system flow control valves FV-20575, FV-20576, FV-20525 and FV-20526 fail as-is and lock upon loss of IAS pressure. Backup air supplies have been installed for these MFW control valves to allow the operators to maintain control capability from the control room following a complete loss of instrument air.

- In addition to the AFW and MFW flow control valves, compressed air bottle backup supplies have been provided for the following critical plant air operated components, i.e.:

  - turbine bypass valves
  - atmospheric dump valves
  - valves providing component cooling water (CCW) to the reactor coolant pumps

The TBVs, ADVs, and CCW valves fail closed upon loss of air pressure.

- The instrument air trouble annunciator in the control room will be modified to provide reflash capability.

- All accumulator tanks have been removed from the IAS, thus eliminating problems with moisture accumulation in the tank bottom from condensation, and concerns regarding noncompliance of the tanks with ASME Code requirements.

- Various air-operated valves that used rubber hoses as supply lines have replaced the rubber hoses (which could degrade as a result of environmental conditions) with stainless steel flex-hose.

- A new cross-tie has been provided between the NGS and the IAS. The existing cross-ties (which were difficult to use and did not have sufficient capacity to supply plant needs) and the associated piping have been capped. Manual operation of the cross-tie is addressed in casualty procedure C.22, "Loss of Plant Air System."

- The letdown filter backflush valve actuators, which leaked air excessively, have been replaced.

- Pressure in the backup air supply bottles could be as high as 2400 psig. Since the main and startup feedwater control valve actuators are only rated for 150 psig maximum air pressure, the licensee will establish the setpoint of the overpressure protection devices at 150 psig.

- A walkdown of the IAS was performed to identify air leaks and to verify agreement between the installed IAS plant configuration and the IAS drawings (e.g., P&IDs). The IAS drawings have been revised where necessary to reflect the current configuration (including all modifications to the IAS).

- Procedures have been established to monitor backup bottle pressure daily, and to initiate appropriate actions if leakage is indicated.

- Periodic test procedures have been established to verify operability of the bottle backup air systems, and procedures have been established for maintenance of air-operated valves.

- Plant operating and casualty procedures have been revised to reflect the new modifications to the IAS with regard to operator actions upon loss of instrument air.

- New operator training programs have been developed to instruct the operators on the new IAS modifications being installed, along with an intensive program on the actions to be taken in a loss of air transient.

- Twenty-five outstanding work requests existing on the IAS and SAS at the time of the December 26, 1985 event have been reviewed by the licensee and prioritized for implementation. As a result of the review, 14 of the 25 work requests have been cited as high-priority items and are scheduled for implementation before plant restart. The remaining 11 work requests are not crucial to IAS/SAS performance, and will be implemented after plant restart.

Three additional items identified by the DFCA are to be considered, although not necessarily before restart, are:

- Review periodic test procedures to ensure the specified tests and their frequencies are consistent with the IAS reliability objectives. In particular, the operability of the backup compressed air bottles and their associated isolating check valves should be inspected/tested approximately quarterly.

- Consider adding backup air bottles to the makeup and seal injection control valves. On loss of the IAS, the failure positions of these valves would result in the makeup tank either slowly filling or draining and require operator attention. In the short term, the operator actions required to control the pressurizer/makeup tank inventories should be clearly delineated in procedures and training programs.

- A number of non-safety-related valve failure positions on loss of the IAS were noted. Although these valves do not directly affect the RCS, the consequences of their failure positions could divert the attention of the operating staff. It is recommended that the required operating staff actions with respect to these valves to be clearly delineated in procedures and training programs. If the specified operator actions significantly tax the operating staff, consider reconfiguring selected valves to fail closed rather than failing open or adding backup air bottles. Specific valves include the retention basin discharge valves, the hotwell makeup valves from the condensate storage tank and the cooling tower makeup valves.

Past degradation/contamination of the IAS at Rancho Seco indicated that additional maintenance and surveillance actions were needed to ensure that the system would operate at a level that would enable plant equipment to function as designed. Most of the failures of air-operated equipment caused by contaminants could have been prevented if the system had been maintained to meet

industry standard ANSI/ISA (Instrument Society of America) Standard S7.3, "Quality Standard for Instrument Air." The level of contamination at which pneumatic equipment performance degrades or fails completely depends upon the equipment's specific design features, operation, and maintenance practices. Operating for long periods of time with a degraded IAS increases the likelihood for common mode failures which could cause the failure of multiple components important to safety. Previous plant IAS maintenance policy would only repair components that had failed or malfunctioned. Efforts are now under way to establish a comprehensive maintenance policy with appropriate procedures for periodic inspection and maintenance of the IAS.

Because the non-safety-related IAS plays a vital role in the proper operation of numerous plant systems/equipment, the effects of IAS failures are not benign. The non-safety-related integrated control system (ICS) at B&W plants similarly plays a vital role in the operation of numerous plant systems/equipment. ICS failures resulting in severe plant transients have been directly attributed to the lack of proper maintenance and surveillance. The licensee should pay particular attention to implementation of a thorough IAS maintenance and surveillance policy that verifies and maintains proper system operation. In addition to proper IAS maintenance and surveillance practices, appropriate plant procedures relating to the loss and restoration of instrument air and adequate operator training are necessary to ensure that safe plant conditions can be readily achieved following IAS losses.

Two existing IAS procedures, A.40, "Plant Air System," and C.23, "Loss of Plant Air," are being revised to provide adequate guidance to the operators for both rapid and slow bleed-down events. The new procedures will address different types of plant air system failures, the use of backup air supplies, and component failure modes and how to restore the system to service. Since a loss of IAS can create situations requiring prompt operator actions that would be difficult to anticipate, it is imperative that operators be well trained and properly guided by emergency operating procedures to respond to loss of IAS events.

In April 1986, the Babcock and Wilcox Owners Group (BWOG) initiated a Safety and Performance Improvement Program (SPIP) with the objective of making generic and plant-specific recommendations designed to reduce the number of reactor trips and complex transients at B&W plants, and to ensure acceptable plant response during those reactor trips and plant transients which do occur. The SPIP reviewed the database again for those systems which have contributed to transient initiation or complexity, and focused attention on those systems that affect OTSG heat transfer (more specifically, those systems that affect OTSG inventory and pressure). On the basis of this review, instrument air systems were selected for detailed evaluation. The objectives of the instrument air system review were to:

- Develop recommendations to improve the reliability of the air supply to critical components required to establish and maintain decay heat removal capability.

- Develop recommendations for design, maintenance and operation of the air system to improve its reliability and to reduce the number and complexity of plant trips caused by air system failures.

The SPIP IAS reviewers concluded that a number of improvements could be made to increase the reliability and operating performance of instrument air systems. Accordingly, the SPIP has made a number of generic and plant-specific recommendations for implementation at B&W plants. The NRC staff intends to issue a separate safety evaluation addressing the adequacy of both the generic and plant-specific BWOG SPIP recommendations pertaining to instrument air systems, and to audit the implementation of the recommendations at B&W plants.

Evaluation

IAS failures have the potential to cause significant plant transients when the control capability for vital components (e.g., main feedwater flow control valves) is lost. A complete loss of the IAS supply (such as could occur because of the loss of the air dryers, compressors, aftercoolers, filters, or receivers) and the failure of individual IAS headers/branch lines (such as could be caused by an accidental severing of a main IAS pipe or a failure of a major coupling) must be considered in evaluating the plant response to IAS failures. Both types of failures have occurred at Rancho Seco during power operation. In November 1986, an outlet flange gasket on one of the air dryers failed, causing a rapid reduction in IAS pressure and the loss of control of the main feedwater flow control vales. When air was restored, the MFW system began to overfeed the OTSGs.

The licensee will modify Rancho Seco IAS before plant restart to improve its reliability and capability to respond to either a sudden or gradual loss of instrument air pressure, and to comply with the guidance of Regulatory Guide 1.68.3. The dedicated diesel-driven air compressor added to the IAS will provide a backup to the existing electric-motor-driven compressors. This added redundancy and diversity in the IAS supply increases the reliability of this portion of the IAS. The Rancho Seco IAS does not include automatic bypass valves around the drier and filter packages to alleviate a loss of air supply. A failure in either of these assemblies could lower the pressure to the point where the diesel-driven compressor automatically starts before an operator could manually bypass the affected components.

A complete loss of air is not considered as likely to occur as a partial pressure loss or losses in branch lines. Loss of air from a distribution header could result in the loss of control or failure of significant plant equipment. The rate and location at which air pressure is lost will determine which components would start to fail first. Instrument air systems are generally not designed as safety systems, and as such, failures of single air system components (e.g., distribution system piping, air dryers, air filters, interconnected air compressors) often cause a total loss of the IAS.

Loss of air to the following equipment will most likely cause an automatic reactor trip (via the reactor protection system), result in operator action to manually trip the reactor, or complicate post-trip recovery actions by the operators:

- main feedwater pumps (pumps trip on loss of air)
- main feedwater valves (valves fail as is on loss of air)
- component cooling water valves to the reactor building (fail closed)
- control rod drive cooling water valves to reactor building (fail closed)

- auxiliary feed flow control valves (fail open)
- atmospheric dump valves (fail closed)
- turbine bypass valves (fail closed)
- main steam to auxiliary steam reducer valve (fails open)
- pressurizer level control valve (fails closed)
- reactor coolant pump seal injection valves (fail open)

The plant response to an IAS pressure loss depends on: (1) the reactor power level and plant mode of operation (hot shutdown, refueling, power. operation, etc.) (2) the type of IAS failure (e.g., total or partial pressure reduction), (3) the location of air failure (branch lines or main header supply) and whether isolation valves are installed to automatically isolate failed branch lines and/or how quickly manual valves can be used, (4) the availability of backup air bottles to hold valves in position, to assist in closing, or provide cycling capacity, (5) the loss-of-air "failure positions" of critical components, (6) availability of backup air compressors, and (7) whether the loss occurs with or without a loss of offsite power.

Hundreds of components use instrument air. However, only a few components can be clearly identified as "critically" influencing the initial plant response to the loss of instrument air (e.g., primary system decay heat removal capability, steam generator inventory, steam pressure, or forced reactor coolant circulation). These "critical" components are those for which a reliable air supply is most important. The air-operated critical components associated with the nuclear steam supply system include:

- makeup control valve
- seal injection control valve
- letdown control valve and other air-operated valves in the letdown path
- makeup line containment isolation valve
- seal injection line containment isolation valve
- seal return line containment isolation valve
- letdown line containment isolation valve
- component (intermediate) cooling water system isolation valve to letdown coolers and reactor coolant pump motors
- turbine bypass valves
- atmospheric dump valves
- main feedwater control valves
- startup feedwater control valves
- auxiliary feedwater flow control valves

- valves in the steam supply to the turbine-driven auxiliary feedwater (TDAFW) pumps
- pneumatic controls for the TDAFW pump
- main steam isolation valves
- various steam extraction line valves and valves to the auxiliary boiler
- service water valves (providing cooling water to the containment heat removal system, etc.).

When the continued operation of certain critical valves is desired/necessary, dedicated backup air reservoirs (bottles) have been installed to automatically provide air when the normal air supply is lost or degraded. The design incorporates a single, pressure-reducing, regulating valve (2400 psig to 85 psig) at each bottle station, installed between the high-pressure bottles and the equipment air lines. The regulators incorporate 175 psig rupture discs. In addition, relief valves set at 120 psig are provided in the air lines downstream of the regulators. Pressure indicators measure the bottle pressure and the header pressure to the valves. A single regulating valve failure could result in the loss of safety function of the associated set of valves. This evaluation did not address the frequency and impacts of regulating valve failures in detail. The December 26, 1985 event did not involve IAS failures.

The IAS modifications to provide the DDAC and backup bottled air supplies for critical components, combined with the other IAS modifications resulting from the DFCA as listed above, should substantially improve the reliability of the IAS. All modifications to the IAS will be tested for both a sudden and a gradual loss of normal instrument air. A functional test will be performed on a component level to verify and document the capabilities of the new modifications.

Upon loss of offsite power, the normal IAS supply will become unavailable. However, some time is involved before the air receivers would depressurize sufficiently to cause air-dependent valves to go to their loss-of-air failure positions. The new DDAC will start automatically upon sensing a low pressure in the normal IAS supply header. Loss of power to the battery charger for the diesel-driven compressor also starts the compressor. Furthermore, dedicated seismic Class 1 high-pressure air bottle backup supplies, with 2-hour capability, will be provided for ICS and EFIC system controlled components such as ADVs, TBVs, MFW, SUFW, and AFW valves. This combination of features helps to ensure that the consequences of a loss of offsite power should not significantly affect the ability to control critical/important components that use instrument air for control or motive power.

The annunciator associated with the IAS has six inputs including low system header pressure, high dewpoint, and high dryer temperature, and will annunciate when the backup air dryers are in use. Failures in the backup diesel-driven air-compressor system will be alarmed via the IDADS in the control room. A separate compressor trouble alarm and compressor running alarm are also provided in the control room. The operator must go to a local control panel to

determine the specific cause for these two alarms. The bottle backup air supplies are provided with low-pressure alarms and status lights in the control room. Setpoints are reached when the remaining supply capacity reaches the 3-hour level. Credit is taken for two hours of modulation capability on loss of the normal air supply. Before these bottles were installed, modulation capability did not exist on loss of air.

Upon a total loss of air, pneumatic control valves will assume their failure positions, and a plant trip will most likely occur. However, if the loss of air is partial or gradual, valves may drift to some intermediate position, or controller setpoints may drift from the desired values. Restoration of air pressure before a plant shutdown is completed may result in a complex event because of the simultaneous "operation" of many safety-related and non-safety-related (control system) components that use instrument air. Casualty procedure C.23 refers to administrative procedure A.40, "Plant Air System," for restoration of plant air. The guidance provided in A.40 does not include precautions for restoring air to critical plant components that may change state when air is restored. The simultaneous operation of air-operated components may further complicate the event and would add to the operators' confusion and workload. Procedure A.40 should be revised to include appropriate precautions for the restoration of instrument air.

The most important activity to improve the reliability of the IAS is to maintain a clean, dry, and oil-free system. In addition, system leakage should be kept as low as practical to reduce the load on the components that compress and condition the air, thereby increasing their reliability by reducing the volume of air processed. Because of the materials and the small clearances of the internal moving parts of pneumatic equipment, clean, dry, and oil-free air is required for reliable, trouble-free operation.

Conclusions

Loss-of-instrument-air transients have been experienced at Rancho Seco. Although shutdown to cold conditions can be achieved without instrument air, manual operation of valves normally operated by instrument air, and other nonroutine operator actions may be required. The licensee has performed a comprehensive evaluation of the IAS, and implemented modifications in equipment and design, and maintenance and testing to improve the reliability of the IAS, to minimize its contribution to the frequency and severity of plant transients. Plant procedures for loss of instrument air transients have been revised.

The staff concludes that the DFCA for the IAS was thorough and comprehensive, and that the modifications to the Rancho Seco IAS discussed above represent a significant improvement in the operability of systems relying on instrument air. These modifications should reduce the frequency of a loss of the IAS (IAS depressurization), reduce the complexity and number of operations that must be performed by the operating staff in the event of IAS depressurization, and better define the manual tasks that must be performed in the event of IAS depressurization. Therefore, the staff concludes that the Rancho Seco IAS as modified is acceptable for plant restart.

3.1.2.5 ICS/NNI System Failure Modes and Effects Analysis

Those aspects of failure modes and effects required for startup are presented in both the Rancho Seco Restart SER and this supplement under headings that address specific systems associated with the ICS/NNI system. A more complete report on the staff evaluation of this issue will be given in another supplement to the Rancho Seco Startup SER to be issued after restart.

3.1.2.6 Loss of Control Room Controls and Indications, Adequacy of Backup Instrumentation

This section describes the effects of loss of integrated control system and non-nuclear instrumentation (ICS/NNI) system power on plant instruments and controls for the ICS/NNI system design existing at the time of the December 26, 1985 event at Rancho Seco, and provides an evaluation of modifications proposed by the licensee to lessen the severity of loss of ICS/NNI power events. An evaluation of the adequacy of backup instrumentation and controls available to the operators to achieve and maintain plant shutdown following a loss of ICS/NNI system power is also provided.

The NNI system is used to measure plant process parameters and to provide corresponding input signals to plant control systems (including the ICS), control room indicators, the plant computer, and the control room annunciator system. Loss of NNI system power typically causes these input signals to fail to midscale values (i.e., the signals become false/invalid and no longer indicate actual plant conditions). Because the ICS is closely coordinated with the NNI system, loss of NNI system power will affect operation of the ICS. The ICS adjusts plant equipment (e.g., main feedwater pumps and valves, turbine bypass valves, control rod position) to match actual process variable values with desired (i.e., demand) values. The NNI system provides the input signals to the ICS that represent the actual values of numerous plant variables. If NNI system power is lost, the ICS will not recognize that its control actions are based upon erroneous signals. The resulting control actions may not be appropriate, and have the potential to introduce a transient throughout the plant. A number of events involving loss of ICS/NNI system power have occurred at B&W plants. Typically, these have resulted in control system malfunctions and significant loss of information to the control room operator.

The NNI system and ICS are not safety-related systems. In general, for each NNI monitored variable, two redundant instrument (transmitter) channels are provided, NNI-X and NNI-Y. Power to the redundant instrument channels is provided by the NNI-X and NNI-Y power systems accordingly. However, a significant number of instruments powered from the NNI-X system provide signals that are conditioned by electronics powered from the NNI-Y system and vice versa (i.e., a number of NNI-X and NNI-Y signals rely on both NNI-X and NNI-Y power, such a loss of either NNI-X or NNI-Y power results in failure of both the NNI-X and NNI-Y signals). Furthermore, many NNI parameters are displayed by a single control room indicator. Therefore, following the loss of either NNI-X or NNI-Y power (referred to as partial loss of NNI power), many of the indications in the primary operating area of the control room are effectively rendered inoperable. The indicators typically fail to mid-scale positions on loss of power, and in many cases the failure positions are not noticeably different from normal operating values. These indicators are routinely monitored by

operators to assess plant status, and to achieve and maintain plant shutdown under normal conditions.

On March 19, 1984, an event occurred at Rancho Seco that involved a partial loss of NNI system power (specifically NNI-X ±24-V dc power). The loss of power was the result of a single failure of an inverter, and undetected drift of an NNI system 24-V dc power supply internal overvoltage protection ("crowbar") circuit setpoint. At the time of the event, the control room indicators that provided essentially all primary and secondary system status information to the operators received inputs from and were powered by the NNI. The loss of power resulted in midscale failures of numerous indicators. The operators manually initiated high pressure injection by procedure, and overpressurized the reactor coolant system to the point where a pressurizer code safety valve opened twice. The loss of NNI power occurred approximately one hour after the reactor had tripped. The ICS responded to the power loss by signaling an atmospheric dump valve (ADV) to open. Since ICS power remained available during this event, the operators were able to place the ADV controls in manual control (taking automatic control of the ADV away from the ICS) to close the valve.

As reported in NUREG-1195, "Loss of Integrated Control System Power and Overcooling Transient at Rancho Seco on December 26, 1985," the event which occurred involved the loss of ICS ±24-V dc power. Upon loss of ICS dc power equipment control modules lost power and provided zero (0-V) dc outputs, and switching relays lost power (going to the de-energized state). This not only caused ICS-controlled equipment to change positions, initiating a plant transient, but also caused the loss of remote manual control of key ICS-controlled plant equipment from the control room. The loss of ICS dc power caused ICS-controlled equipment to respond in the following manner, as designed:

- The turbine bypass valves (TBVs), atmospheric dump valves (ADVs), the main feedwater (MFW) main and startup flow control valves, and the auxiliary feedwater (AFW) flow control valves went to the 50% open position.
- The MFW stop (block) valves closed.
- The MFW pump turbines decreased to minimum speed.
- The MFW flow recorders operated from the ICS went to the mid-scale position (indicating false MFW flow to the steam generators when the actual flow was zero).
- The reactor control rods remained "as-is."
- The auxiliary steam reducing station setpoint went to the mid-scale value causing the auxiliary steam header relief valves to open.

The incident at Rancho Seco on December 26, 1985 was significant because it again demonstrated that a single failure in the non-safety-related ICS/NNI could subject the plant to an undesirable transient. The licensee has proposed to make hardware modifications to the ICS/NNI system, and procedural changes before restart to reduce the severity of such a transient and the resulting burden it could cause on the operators. The hardware modifications are discussed below. The procedural changes are discussed in Section 3.1.2.10 of this report, "Operator Response Procedures."

Plant Modifications To Reduce the Consequences of Loss of ICS/NNI System Power Events

The licensee has modified hardware to ensure that plant conditions will stabilize after a loss-of-ICS/NNI-power transient, and to ensure that the plant response to restoration of power will not complicate recovery from the transient. The modifications are designed to provide the capability to establish controlled heat removal from the reactor coolant system (RCS) following a loss of ICS and/or NNI ac or dc power by automatically placing the plant in the B&W Owners Group anticipated transient operating guidelines (ATOGs) "post-trip" window (i.e., a known safe state as defined by the emergency operating procedures, EOPs). The primary function of the control room operator will be to verify that the automatic actions (trip of the main feedwater pumps and automatic initiation of auxiliary feedwater by the emergency feedwater initiation and control system) have occurred, and that stable plant conditions are achieved within the "post-trip" window.

The post-trip window is part of the safety parameter display system (SPDS) "post-trip" display (see Figure 3.23). By maintaining the RCS pressure-temperature (P-T) relationship within an identified range, the operator is assured that the plant is in a known safe condition. If the SPDS display shows that the actual P-T relationship is outside of the post-trip window, then operator would be required to stabilize the plant manually. The EOPs will provide guidance for operator action through the use of backup instrumentation and controls that are unaffected by the ICS/NNI power loss. The staff's evaluation of the adequacy of backup instrumentation and controls that can be used by the control room operator to safely control and stabilize the plant within the post-trip window, and to achieve subsequent safe plant shutdown following a loss of ICS/NNI power, is provided below.

The licensee has modified the ICS/NNI power system design so that a loss of NNI-X, NNI-Y, or NNI-Z dc power, or loss of NNI-X or NNI-Y ac power will result in a forced automatic trip of the ±24-V dc ICS power supplies. This will allow the control room operator to concentrate on a common response (i.e., loss of ICS dc power) for any ICS/NNI power failure. The automatic ICS dc power trip circuitry is discussed in Section 3.1.2.2 of this report, "Loss of ICS/NNI System dc Power." To ensure that the plant goes to a known safe state, the licensee has installed circuitry to automatically trip the main feedwater (MFW) pump turbines on loss of ICS ac or dc power. The trip of both MFW pumps will in turn cause a reactor trip. Circuitry to initiate reactor trip on MFW pump trip was previously installed in accordance with TMI Action Plan Item II.K.2.10, "Safety Grade Anticipatory Reactor Trip," of NUREG-0737, "Clarification of TMI Action Plan Requirements." The operators are trained to initiate AFW flow to the once-through steam generators (OTSGs) upon receipt of ICS/NNI power failure alarms and MFW pump trip alarms. In the absence of operator action, the newly installed safety-related emergency feedwater initiation and control (EFIC) system will automatically initiate AFW flow to the OTSGs upon detecting a low water level, and will control OTSG level and pressure. A detailed evaluation of the EFIC design is provided in Section 3.1.3 of this report, "Emergency Feedwater Initiation and Control System." The licensee has stated that it is preferable to promptly trip the MFW pumps to reduce steam drain and to reduce the likelihood of unintended steam generator (SG) feeding (thus providing protection against OTSG overfeeding/overcooling), and to set the

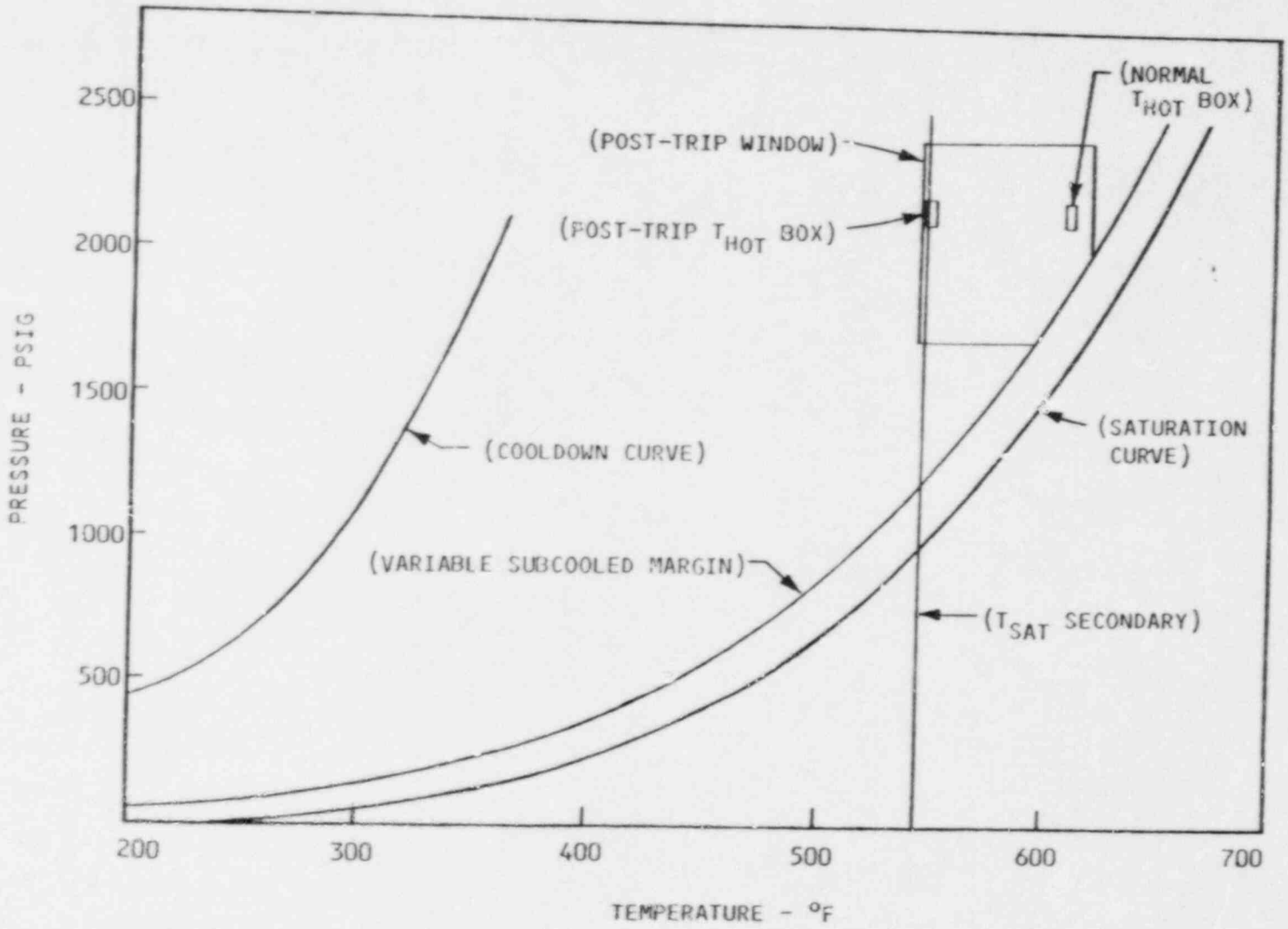


Figure 3.23 Safety parameter display system pressure-temperature "post-trip" window display

stage for the safety-related EFIC and AFW systems to become the source of water to the OTSGs.

The circuitry installed to automatically trip the MFW pumps is shown in Figure 3.24, and consists primarily of undervoltage relays used to sense the loss of ICS 120-V ac power, and relays used to sense the loss of ICS ±24-V dc power. The relay contacts are then used to energize the trip solenoids for both MFW pumps. The same trip solenoids are actuated separately by the existing MFW pump trip circuitry. ICS 120-V ac power is sensed downstream of the automatic bus transfer (ABT) devices. Time delay on dropout (TDD) relays are provided to delay trip of the MFW pumps for 1 second following loss of ICS 120-V ac power to allow time for the automatic transfer to occur (the transfer should occur within 0.5 second). The trip logic is arranged in a two-out-of-two configuration to minimize the probability of spurious MFW pump trips due to a single failure. A status light has been mounted on the front of the ICS cabinets to indicate a half-trip condition such as could be caused by failures within the added circuitry. The light is on only when all relays are in the untripped/energized state (i.e., when all ICS ac and dc power is available). Periodic observation of the indicating light will permit early detection of a half-trip condition. The added MFW pump trip circuits are not safety related. Testing will be performed during plant startup to verify that trip of the MFW pumps occurs on loss of ICS ac and dc power as designed, and the circuits will be functionally tested during each refueling outage thereafter.

The staff believes that the licensee's approach of implementing design changes to dictate the plant response to ICS/NNI system power failures (i.e., to ensure the plant attains a known safe state by causing a trip of the MFW pumps reactor trip, and automatic initiation of AFW), thus allowing the operators to focus on a common plant response through specific procedures on which they have been trained, is a good approach and should result in a significant reduction in the severity of loss of ICS/NNI system power transients.

Should the MFW pump speed control fail "as-is" on loss of ICS dc power (i.e., a failure occurs in the automatic MFW pump trip circuits), the control room operator will have the capability to manually trip the pumps or to manually initiate EFIC system isolation of MFW to prevent continued main feedwater flow to the OTSGs. Such action will be controlled on the basis of the EOPs. The licensee has confirmed that trip of the MFW pumps can be verified via annunciator windows on control room panel H2YSB and that the operators will be trained to use such indication upon loss of ICS power. The annunciator windows and associated circuits are verified to be operable every two years in accordance with preventive maintenance tasks. The MFW pump turbine manual trip circuits are not safety related and are tested for operability every two years in accordance with routine administrative procedures. The manual controls are located on control room panel H1SS.

On loss of ICS dc power, the MFW flow control valve and startup control valve will continue to fail to the 50% open position as a function of the ICS ±10-V dc control module circuitry. The MFW block valves, downstream of the MFW flow control valves, will continue to receive a "close" signal as a result of deenergization of the ICS switching relays upon loss of ICS dc power. This would isolate the 50% failed-open MFW flow control valves. However, the loop A and loop B startup control valves are located in a parallel flow path around

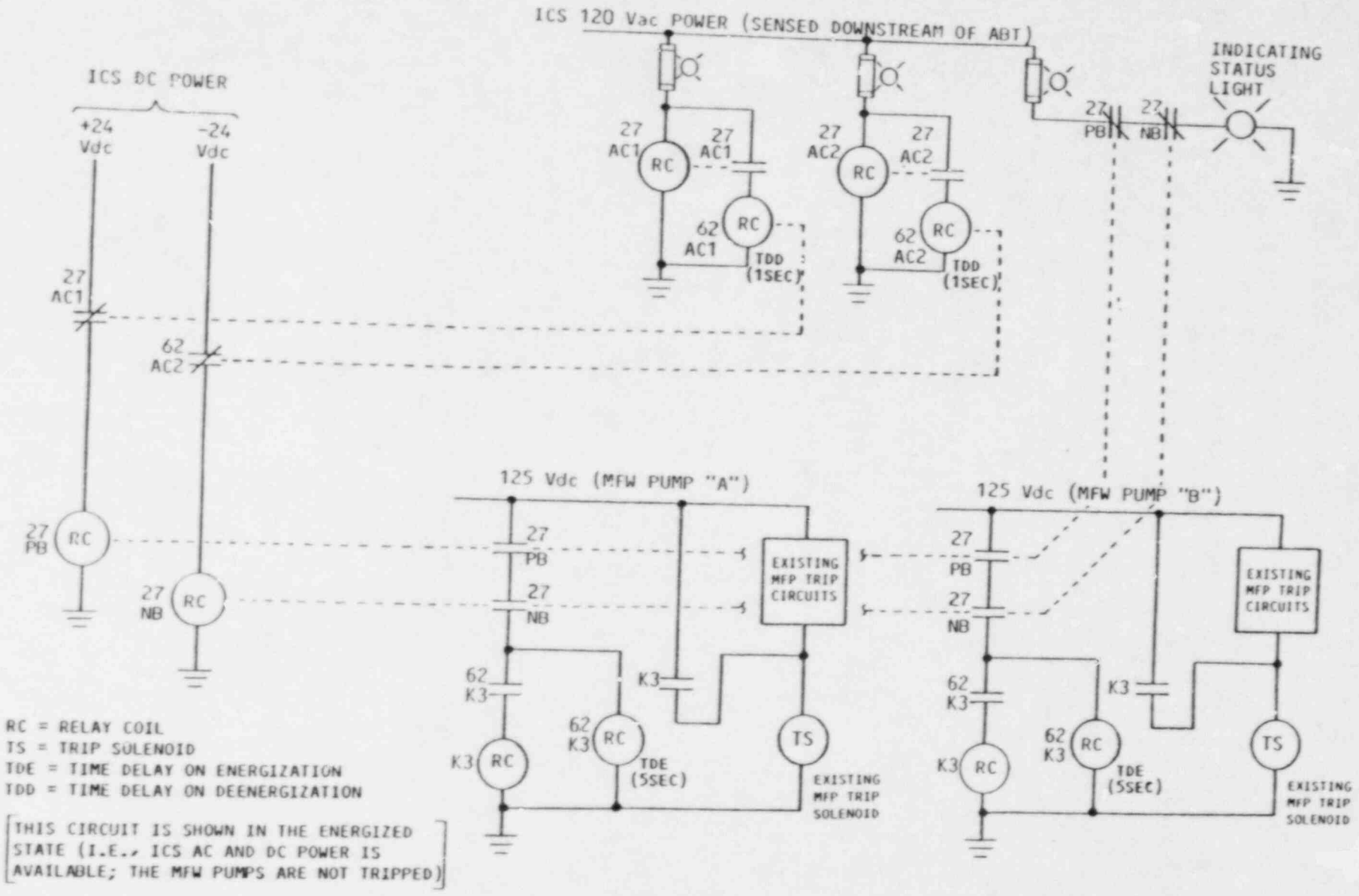


Figure 3.24 Automatic trip of the main feedwater pumps on loss of ICS ac or dc power

the MFW block valves, and hence will not be isolated by closure of the block valves. The licensee has, therefore, provided a series MFW isolation valve downstream of the MFW flow control and startup control valves which will be controlled by the EFIC system. Closure of this valve will prevent unintended feeding of the OTSGs by the condensate pumps. The EFIC system also provides safety related automatic and manual isolation capability for the MFW flow and startup control valves and MFW block valves. The EFIC system isolation signals, if present, will override the ICS control signals to these valves. EFIC system automatic isolation of the MFW system valves will be initiated either from low SG pressure or high-high SG level. The EFIC system is independent of ICS/NNI power.

Control room position indication for the MFW isolation and block valves will be safety related whereas the MFW control and startup valves will have non-Class 1E position indication. The indication for these valves is located on panel H1RI in the control room, and will be tested for operability during each refueling outage as part of valve full stroke testing in accordance with the Technical Specifications.

Four specific ICS-controlled devices were identified by the licensee that could, if improperly positioned, individually take the plant out of the post-trip window. This concern is identified in NUREG-1195. The devices are:

- AFW flow control valves
- atmospheric dump valves
- turbine bypass valves
- auxiliary steam control system

On the basis of this finding, the licensee has proposed corrective actions designed to ensure that these devices will not prevent a known safe state from being achieved following a loss of ICS/NNI system power. In general, the devices have been made either partially or totally independent of the ICS as described below. Control of the AFW system (including the AFW flow control valves) and control of atmospheric dump valves (ADVs) has been removed from the ICS and will now be performed by the EFIC system.

Three ADVs are provided on each main steamline. Two of the three ADVs per steamline are normally blocked during reactor operation via upstream local manually operated valves. The licensee has added motor-operated isolation valves upstream of the unblocked ADVs to provide the operator with the capability to isolate a stuck-open ADV to prevent an uncontrolled steam release that could result in overcooling of the primary system. EFIC system control of the ADVs is discussed in Section 3.1.3 of this report. The manual control circuits for the ADVs (six total) and the ADV motor-operated isolation valves (two total) are safety related and will be functionally tested monthly in accordance with the Technical Specifications (TS). Control room position indication for the ADVs will be classified as not safety related. Two means of position indication are provided: limit switch contact outputs to red/green status lights, and acoustic monitor outputs to the interim data acquisition and display system (IDADS). The IDADS is a plant process computer system that monitors plant conditions and performs various calculation, trending, alarm, indication, and post-transient data logging functions. The ADV motor-operated isolation valves will have Class 1E position indication in the control room.

The position indication circuits for the ADVs and ADV isolation valves will also be verified operable monthly per TS during valve full-stroke tests. The manual control switches and valve position indication status lights for the ADVs and the ADV isolation valves will be located on control room panel H1RI and H2YS respectively. Since the ADV and ADV isolation valve control circuits will be powered independent of the ICS and NNI system, loss and/or restoration of ICS/NNI system power will not affect these valves.

EFIC system automatic and manual control of the AFW system flow control and isolation valves is discussed in Section 3.1.3 of this report. Proper control of AFW flow is necessary to ensure controlled heat removal from the reactor following MFW pump trip and reactor trip upon loss of ICS/NNI system power. The AFW flow control valves (FV-20531, FV-20527, FV-20532, and FV-20528) can be operated manually from the control room using safety-related control circuits powered independent of ICS/NNI system power. Safety-related position indication will be provided in the control room for each of the AFW flow control and isolation valves. The control switches and valve position indication will be provided on control room panel H1SS(E). The manual control circuits and valve position indication will be functionally tested monthly to verify operability in accordance with the TS.

The four turbine bypass valves (TBVs) will remain under normal ICS control, but have been modified so that they will be signaled to automatically go to the fully closed position upon loss of ICS dc power (instead of going to the 50% open position as occurred during the December 26, 1985 event) to prevent excessive steam flow that could lead to overcooling. The ICS provides a ±10-V dc signal used to control the TBVs. This voltage signal will be processed through a voltage-to-current (E/I) converter to provide a 4-20-mA control output current to the TBVs (a +10-V dc signal causes a 20-mA output that opens the valves, and a -10-V dc signal causes a 4-mA output that closes the valves). The E/I converters will be powered from the ICS ±24-V dc supplies. When the TBVs are under normal ICS control, a loss of ±24-V dc ICS power to the E/I converter will result in a zero output (representative of a 4-mA condition) causing the TBVs to close. It should be noted that upon restoration of ICS power, a memory module upstream of the E/I converter will power-up low (i.e., reinitialize to -10 V dc) thereby ensuring that the TBVs remain closed. Manual operator action is required after the restoration of ICS power to return the TBVs to automatic ICS control.

If the TBVs have "failed-closed" because of loss of ICS power, the EFIC system will control OTSG pressure through the ADVs. The upstream main steam safety valves (MSSV) provide OTSG overpressure protection. The licensee has stated that the TBVs are not required to maintain reactor coolant system pressure and temperature control for safe plant shutdown. However, the operator will be provided with the capability to bypass the automatic ICS closure signal to the TBVs, via newly installed control selector switches. Two Bailey manual TBV control stations, H1C-20561 and H1C-20564, that use an alternate battery-backed power supply to allow manual control independent of the ICS have been installed on control room panel H1RI. The manual selector switches are two-position switches that allow for either of two modes of TBV operation, "NORMAL" ICS control or "LOSS OF ICS" power control. The "LOSS OF ICS" control mode will allow the operator to open the TBVs to pass steam to the condenser when ICS power is lost by providing a separate 4-20-mA control signal to the TBVs.

Indication is provided on the manual controller to signal the operator that control has been transferred via the selector switch. The operator will be able to operate the TBVs through the Bailey manual control station circuit only if condenser interlocks are satisfied (i.e., condenser vacuum and condenser cooling water are available). The manual control station will be set for zero output when it is not being used to control the TBVs (i.e., when the selector switch is in "Normal" position). The manual control circuits are not dependent on the availability of ICS/NNI system power. The TBV control circuits and the position indication are not Class 1E. The subject circuits will be verified operable on a quarterly basis in accordance with the TS during valve full-stroke tests.

Two motor-operated isolation valves have been installed upstream of the TBVs with manual control from the control room to provide OTSG isolation capability should the TBVs fail to close. The two valves will isolate main steam flow from the A and B steam generators to TBVs PV-20561/PV-20563 and TBVs PV-20564/PV-20566, respectively. The manual controls including position indication for the TBV motor-operated isolation valves are classified as safety related and are located on control room panel H2YS.

The valve position indication provided in the control room for the TBVs, ADVs, AFW flow control valves, and MFW flow control and startup valves are powered independent of the ICS and NNI system. Such valve position indication is important to safe plant shutdown because it will assist the operator in diagnosing a possible stuck or mispositioned valve. Position indicating status lights have been added to panel H1RI (for the ADVs, TBVs, MFW flow control, and startup valves) and to panel H1SS(E) (for the AFW flow control valves). There is one red and one green status light for each valve. The lights function as follows:

OPEN	When the valve is not in the full-closed position, the red light will illuminate.
CLOSED	When the valve is not in the full-open position, the green light will illuminate.
INTERMEDIATE	When the valve is in an intermediate position, both lights will illuminate.

The auxiliary steam reducing station normally obtains its steam from the main steam system following a turbine trip. During the December 26, 1985 event, the loss of ICS power resulted in overpressurization of the auxiliary steam header which caused the auxiliary steam system safety relief valves to lift. This contributed to the overcooling of the plant through the depressurization of the main steam lines. Auxiliary steam is needed following a reactor trip for plant services such as condenser air ejectors and turbine shaft seals. Therefore, the licensee has decided to retain this feature under normal ICS control with the added capability to manually throttle the supply independent of the ICS when desired. The design change involves the removal of the existing ICS electronic pressure control components and the installation of a new pneumatic pressure controller with remote setpoint adjustment through the ICS. The remote setpoint adjusted using an electric-motor-driven regulator (powered from the 120-V ac ICS supply) which will deliver a 3-to-15-psig signal to the pressure

controller. The design will be such that a loss of ICS power will cause the setpoint regulator to maintain its existing pneumatic output to the controller at a constant value (i.e., remains at previous setpoint). This will maintain the amount of existing steam flow and eliminate the header overpressure conditions that have occurred in the past. It will be possible to continue modulating the auxiliary steam pressure control valve independent of the ICS controlled pressure regulator through the manipulation of an auto/manual station within the pneumatic pressure controller. The auto/manual control station is located in the turbine building near the control valve area and will override the setpoint adjustment provided by the ICS-controlled auxiliary steam demand station located in the control room (panel H2X).

The above modifications to prevent adverse equipment response to ICS/NNI system power losses, and to ensure that ICS/NNI system power failures do not result in the loss of both automatic and remote manual control of plant equipment, should significantly reduce the consequences of ICS/NNI system power failures, and decrease the burden on the operators during recovery from loss of ICS/NNI system power events.

Instrumentation Available Following a Loss of ICS/NNI System Power

The staff reviewed the backup instrumentation and controls used by the control room operators to control and shut down the plant following a loss of ICS/NNI system power. The licensee's approach, as reflected through design changes, operator training, and procedures, is to focus on the need for establishing stable plant conditions before making any attempt to restore ICS/NNI system power. Emergency operating procedure E.02, "Vital System Status Verification," provides guidance for obtaining stable plant conditions following a reactor trip, and includes instructions for verifying that stable plant conditions have been attained. Procedure E.02 contains caution statements concerning backup instrumentation to be used to monitor plant status should ICS/NNI system power be lost. It should be noted that the licensing basis for Rancho Seco does not include compliance with BTP RSB 5-1 (NUREG-0800). BTP RSB 5-1 requires that the plant design allow for the reactor to be taken from normal operating conditions to cold shutdown using only safety-related equipment/systems. However, consistent with the licensing basis, some non-safety-related ICS/NNI system instrumentation and controls are normally used to achieve plant shutdown. The Rancho Seco approach for control and shutdown of the plant following a loss of ICS/NNI power also allows the operators to use non-safety-related as well as safety-related controls and indications.

The control room operators will be trained to use the SPDS, EFIC system, IDADS, and newly installed multiplant trend recorder indications when responding to a transient resulting from or associated with a loss of ICS/NNI system ac or dc power. The licensee has stated that the information supplied by these systems/instruments is sufficient to verify that the plant has been stabilized at hot shutdown. Procedure E.02 references the use of the SPDS, IDADS, and EFIC system displays upon loss of NNI system power. Should the ICS/NNI system power recovery effort be unsuccessful after obtaining stable, hot shutdown conditions, the dedicated multi-plant trend recorder (located on control room panel H1CO) will be available for use in maneuvering the plant to cold shutdown. The SPDS and IDADS will use computer-based CRT displays, whereas the EFIC system and

multi-plant trend recorder will provide hard-wired indication. The EFIC system indication is provided on panel H1SS(E) and is safety related.

On loss of ICS and/or NNI system power, procedures and training will direct the operator(s) to ignore all ICS and NNI system indication. To allow the operator to quickly distinguish between indications dependent on ICS/NNI power (that could provide false/invalid information on power failure), and indications that are independent of the ICS/NNI system (and therefore should be available for use following ICS/NNI system power losses), all ICS and NNI system hard-wired indicators and recorders will be clearly labeled. Purple ICS and orange NNI system tags have been placed on all ICS/NNI system instrumentation to allow the operator to determine which instruments are not reliable when failure of ICS or NNI system power is annunciated. The colored labels will contain the abbreviation "ICS" and/or "NNI." The colors were chosen following human factors practices. The letter sizes will be 0.15 inch for quick identification. Some indicators receive both ICS and NNI system conditioned signals and will, therefore, have a split label with both colors and system designations.

The licensee was asked to provide a complete list of control room ICS/NNI system-dependent indications and controls, and for each item on the list, to identify (1) whether the instrument/control is used to achieve hot and/or cold shutdown, (2) the alternate/backup equipment that is not dependent on ICS/NNI system power, and therefore, will be available to the control room operators following a loss of ICS/NNI system power, and (3) the surveillance performed on the backup instruments and controls to periodically verify their operability to ensure they would be available if needed. This information is provided in Table 3.3. Upon reviewing this information, it appears that sufficient alternate equipment is provided to the control room operators to achieve and maintain plant shutdown. As can be seen from Table 3.3, backup instrumentation independent of the ICS/NNI system does not exist for many indications and controls. However, for each instance where an ICS/NNI system indication or control is used by the operators to bring the plant to a hot-shutdown or cold-shutdown condition, a backup indication or control independent of the ICS and NNI system is provided.

The SPDS will indicate, independent of ICS and NNI, parameters required for hot shutdown on two independent color monitors. All SPDS inputs can be shown on either monitor (i.e., channel A data can be called up on the channel B monitor and vice versa). Information will be provided to the operator via displays selected by the operation of a single pushbutton on the SPDS control panel. The staff understands that following a plant trip, the SPDS will automatically switch to the "post-trip" window display. The operators will use this information for trending RCS pressure and temperature and for determining the appropriate emergency procedure to follow. All Regulatory Guide (RG) 1.97, Category 1 variables will be presented on the SPDS "post-trip" display. The licensee has committed to revise the SPDS (including the video monitors) to meet the requirements applicable to RG 1.97, Category 1 instrumentation. This includes seismic qualification, separation (cable routing), isolation, and Class 1E power supply requirements. The overall design evaluation of the SPDS upgrade for Rancho Seco is provided in Section 4.6 of this SSER.

The IDADS, including displays, is not safety related. This system will consist of two CRT displays located diagonally across from each other in the control

Table 3.3 (Page 1) Backup (alternate) indications and controls used by the control room operators following a loss of ICS/NNI power

Non-safety-related indications and controls in the control room that become inoperable upon loss of ICS/NNI power	Safety classification and location		Indications and controls used to achieve plant shutdown		Periodic surveillance testing to verify operability of backup indications and controls	
	Safety related	Not safety related	Hot shutdown	Cold shutdown	Frequency	Control document
OTSG A level (Operate range) (Startup range) (Wide range) · IDADS · Bailey 855	· SPDS (Full range) (Operate range) (High range) · H1SS (EFIC)	· H4BS · IDADS · H1CO (Wide range) · H2SD	Yes	Yes	18 mos.	· Technical Spec. (H1SS) · Admin. Controls (SPDS) (IDADS) (H2SD) (H1CO) (H4BS)
OTSG B level (Operate range) (Startup range) (Wide range)	Same as for OTSG A level	Same as for OTSG A level	Yes	Yes	18 mos.	Same as for OTSG A level
OTSG A pressure · SPDS · IDADS · Bailey 855	· H1SS · SPDS	· H4BS · H1CO · H2SD	Yes	Yes	12 mos.	Admin. Controls (H4BS) (H1CO) (SPDS) (H1SS) (H2SD)
OTSG B pressure · SPDS · IDADS · Bailey 855	Same as for OTSG A pressure	Same as for OTSG A pressure	Yes	Yes	12 mos.	Same as for OTSG A pressure
Reactor coolant outlet temp. (T_h) - loop A, loop B · IDADS · Bailey 855	· SPDS	· IDADS · H4BS · H1CO · H2SD (Remote shutdown panel)	Yes	Yes	18 mos.	Admin. Controls (IDADS) (H4BS) (H1CO) (SPDS) (H2SD)

Table 3.3 (Page 2)

Non-safety-related indications and controls in the control room that become inoperable upon loss of ICS/NNI power	Safety classification and location		Indications and controls used to achieve plant shutdown		Periodic surveillance testing to verify operability of backup indications and controls	
	Safety related	Not safety related	Hot shutdown	Cold shutdown	Frequency	Control document
Reactor coolant inlet temp. (T_c) - loop A, loop B - IDADS - Bailey 855	None	- IDADS - H4BS - H1CO - SPDS - H2SD (Remote shutdown panel)	Yes	Yes	12 mos.	Admin. Controls (IDADS) (H4BS) (H1CO) (SPDS) (H2SD)
Core flood tank A level - IDADS - Bailey 855	- SPDS	- IDADS	No	No	18 mos.	- Admin. Controls (SPDS) - Technical Spec.
Core flood tank B level - IDADS - Bailey 855	- SPDS	- IDADS	No	No	18 mos.	- Admin. Controls (SPDS) - Technical Spec.
Core tank A pressure	None	None	No	No	18 mos.	Technical Spec.
Core tank B pressure	None	None	No	No	18 mos.	Technical Spec.
Reactor coolant makeup tank level - IDADS - Bailey 855	None	- IDADS - H4BS - H1CO - SPDS - H2SD (Remote shutdown panel)	Yes	Yes	18 mos.	- Technical Spec. - Admin. Controls (IDADS) (H4BS) (H1CO) (SPDS) (H2SD)
Reactor coolant makeup flow	None	- H1CO - SPDS	Yes	Yes	12 mos.	Admin. Controls (H1CO) (SPDS)
Reactor coolant letdown flow - IDADS - Bailey 855	None	- IDADS - H1CO - SPDS	Yes	Yes	12 mos.	Admin. Controls (IDADS) (H1CO) (SPDS)

Table 3.3 (Page 3)

Non-safety-related indications and controls in the control room that become inoperable upon loss of ICS/NNI power	Safety classification and location		Indications and controls used to achieve plant shutdown		Periodic surveillance testing to verify operability of backup indications and controls	
	Safety related	Not safety related	Hot shutdown	Cold shutdown	Frequency	Control document
Decay heat system A flow	· SPDS	· IDADS	No	Yes	18 mos.	· Admin. Controls (SPDS) · Technical Spec.
Decay heat system B flow	· SPDS	· IDADS	No	Yes	18 mos.	· Admin. Controls (SPDS) · Technical Spec.
Pressurizer level · IDADS · Bailey 855	· SPDS	· IDADS · H4BS · H1CO · H2SD	Yes	Yes	18 mos.	· Technical Spec. · Admin. Controls (IDADS) (H4BS) (H1CO) (SPDS) (H2SD)
Reactor coolant system A pressure	· SPDS	· H4BS · H1CO · H2SD (Remote shutdown panel) · IDADS	Yes	Yes	6 mos.	· Technical Spec. · Admin. Controls (H4BS) (H1CO) (H2SD) (SPDS) (H2SD)
Reactor coolant system B pressure	· SPDS	· H4BS · H1CO · H2SD (Remote shutdown panel) · IDADS	Yes	Yes	6 mos.	· Technical Spec. · Admin. Controls (H4BS) (H1CO) (H2SD) (SPDS) (H2SD)
Pressurizer temperature · IDADS · Bailey 855	· SPDS	· IDADS	No	No	18 mos.	· Technical Spec. · Admin. Controls (SPDS) (IDADS)
Reactor coolant system loop A flow	None	· SPDS (Total flow)	No	No	N/A	N/A

Table 3.3 (Page 4)

Non-safety-related indications and controls in the control room that become inoperable upon loss of ICS/NNI power	Safety classification and location		Indications and controls used to achieve plant shutdown		Periodic surveillance testing to verify operability of backup indications and controls	
	Safety related	Not safety related	Hot shutdown	Cold shutdown	Frequency	Control document
Reactor coolant system loop B flow	None	· SPDS (Total flow)	No	No	N/A	N/A
Reactor coolant system loop A dT · SPDS · IDADS	None	None	No	No	N/A	N/A
Reactor coolant system loop B dT · SPDS · IDADS	None	None	No	No	N/A	N/A
Unit T_{ave}	None	None	No	No	N/A	N/A
Loop A T_{ave}	None	None	No	No	N/A	N/A
Loop B T_{ave}	None	None	No	No	N/A	N/A
Reactor coolant system pressure (low range) · SPDS	None	None	No	No	N/A	N/A
Reactor coolant pump seal pressure · IDADS · Bailey	None	None	No	No	N/A	N/A
Reactor coolant makeup tank pressure	None	None	No	No	N/A	N/A
Reactor coolant system makeup pressure	None	None	No	No	N/A	N/A
Letdown temperature	None	None	No	No	N/A	N/A

Table 3.3 (Page 5)

Non-safety-related indications and controls in the control room that become inoperable upon loss of ICS/NNI power	Safety classification and location		Indications and controls used to achieve plant shutdown		Periodic surveillance testing to verify operability of backup indications and controls	
	Safety related	Not safety related	Hot shutdown	Cold shutdown	Frequency	Control document
Decay heat loop A temperature	None	- Bailey 855* - IDADS	No	Yes	None	N/A
Decay heat loop B temperature	None	- Bailey 855* - IDADS	No	Yes	None	N/A
Main FW valve A ΔP - IDADS - Bailey 855	None	None	No	No	N/A	N/A
Main FW valve B ΔP - IDADS - Bailey 855	None	None	No	No	N/A	N/A
Main FW loop A flow - SPDS - IDADS - Bailey 855	None	None	No	No	N/A	N/A
Main FW loop B flow - SPDS - IDADS - Bailey 855	None	None	No	No	N/A	N/A
Startup FW loop A flow - IDADS - Bailey 855	None	None	No	No	N/A	N/A
Startup FW loop B flow - IDADS - Bailey 855	None	None	No	No	N/A	N/A

*IC input directly into Bailey computer.

Table 3.3 (Page 6)

Non-safety-related indications and controls in the control room that become inoperable upon loss of ICS/NNI power	Safety classification and location		Indications and controls used to achieve plant shutdown		Periodic surveillance testing to verify operability of backup indications and controls	
	Safety related	Not safety related	Hot shutdown	Cold shutdown	Frequency	Control document
PRT temperature	None	H2X (Component cooling water outlet temp.)	No	Yes	12 mos.	Admin. Controls (H2X)
PRT pressure	None	H2PS (PI21920)	No	Yes	18 mos.	Admin. Controls (H2PS)
Neutron error	None	None	No	No	N/A	N/A
Generator frequency	None	None	No	No	N/A	N/A
Makeup filter ΔP	None	- H1CO	No	No	24 mos.	Admin. Controls (H1CO)
Secondary steam temperature (loop A) - IDADS - Bailey 855	None	- H1CO	No	Yes	12 mos.	Admin. Controls (H1CO)
Secondary steam temperature (loop B) - IDADS - Bailey 855	None	- H1CO	No	Yes	12 mos.	Admin. Controls (H1CO)
Main FW flow (loop A)	None	None	No	No	N/A	N/A
Main FW flow (loop B)	None	None	No	No	N/A	N/A
Main FW flow (Startup range) (loop A)	None	None	No	No	N/A	N/A
Main FW flow (Startup range) (loop B)	None	None	No	No	N/A	N/A

Table 3.3 (Page 7)

Non-safety-related indications and controls in the control room that become inoperable upon loss of ICS/NNI power	Safety classification and location		Indications and controls used to achieve plant shutdown		Periodic surveillance testing to verify operability of backup indications and controls	
	Safety related	Not safety related	Hot shutdown	Cold shutdown	Frequency	Control document
Main fw temperature (loop A)	None	None	No	No*	N/A	N/A
Main fw temperature (loop B)	None	None	No	No*	N/A	N/A
Power range	None	None	No	No	N/A	N/A
Total FW flow	None	None	No	No	N/A	N/A
Average main FW temperature	None	None	No	No	N/A	N/A
Main steam header pressure	None	None	No	No	N/A	N/A
Pressurizer heaters	None	None	No	No**	N/A	N/A
Reactor coolant pump seal injection	None	None	No	No**	N/A	N/A
Letdown flow	None	None	No	No**	N/A	N/A
Power-operated relief valves (PORVs)	None	None	No	No*	N/A	N/A
Makeup flow	None	None	No	No*	N/A	N/A
Turbine bypass valves loop A	None	- H2SD - H1RI	No	No	18 mos.	Admin. Controls (H2SD) (H1RI)

*For a normal cooldown, MFW may be used; but on loss of ICS/NNI, MFW pumps are tripped.
**For a normal cooldown, this control may be used; but the failed position during a loss of ICS/NNI still allows cooldown without this control.

Non-safety-related indications and controls in the control room that become inoperable upon loss of ICS/NNI power	Safety classification and location		Indications and controls used to achieve plant shutdown		Periodic surveillance testing to verify operability of backup indications and controls	
	Safety related	Not safety related	Hot shutdown	Cold shutdown	Frequency	Control document
Turbine bypass valves loop B	None	- H2SD - H1RI	No	No	18 mos.	Admin. Controls (H2SD) (H1RI)
Main FW loop A valves (Control) (Startup) (Block)	None	None	No	No*	N/A	N/A
Main FW loop B valves (Control) (Startup) (Block)	None	None	No	No*	N/A	N/A
Main FW loop A pump	None	None	No	No**	N/A	N/A
Main FW loop B pump	None	None	No	No**	N/A	N/A
Auxiliary steam reducing station	None	H2X	No	No	24 mos.	Admin. Controls (H2X)
Generator pulser	None	None	No	No	N/A	N/A
Control rod drives	None	None	No	No	N/A	N/A
Turbine EHC	None	None	No	No	N/A	N/A

*For a normal cooldown, this control may be used; but the failed position during a loss of ICS/NNI still allows cooldown without this control.

**For a normal cooldown, MFW control may be used; but on loss of ICS/NNI, MFW pumps are tripped.

room. Although the IDADS was available during the December 26, 1985 event and performed well by providing a comprehensive view of the sequence of events and plant conditions, a specific concern related to the IDADS sample rate was identified during investigation of the event. The post-trip review of the IDADS alarm printout revealed that steam generator pressure was approximately 370 psig when the main steamline failure logic (MSLFL) system alarmed. The pressure setpoint was set to alarm at 435 psig. The licensee's ensuing analysis and followup troubleshooting determined that the MSLFL inputs to the IDADS were being monitored once-per-minute. During the period of interest, OTSG pressure was decreasing approximately 70 psig per minute. Hence, the MSLFL did not alarm until the pressure was much lower than the setpoint because the IDADS sample rate was too slow.

Installation of the new EFIC system will replace the MSLFL in its entirety and the EFIC system will perform the same main feedwater isolation function originally performed by the MSLFL. The low OTSG pressure setpoint will be changed from 435 psig to 600 psig, as it was determined by analysis that a higher setpoint is desirable to ensure that the condensate pumps will not begin feeding a depressurized OTSG. The EFIC annunciated points and analog process values will be available on IDADS as part of the plant trip history logging and will be potentially useful for off-line evaluations of any anomalous EFIC behavior. The IDADS scan rate for the EFIC system analog process variables (OTSG pressure, OTSG level and feedwater flow) will initially be once per second (fastest scan rate for IDADS). The licensee has stated that it may propose to use a less frequent scan rate later if sufficient similar indications are available for post-accident analysis.

The staff questioned the use of the SPDS and IDADS computerized systems to achieve and maintain a safe plant status following loss of ICS/NNI system power events because some inputs (indications) to these systems depend on the NNI system for power. Through discussions with the licensee, the staff understands that the SPDS will use an "(N)" designation beside those parameters which are NNI dependent, allowing the operators to recognize the dependance and avoid reliance on these indications. However, the staff is not aware of plans to provide a similar special designation for the IDADS indications dependent on NNI power. Step 12.1 of procedure E.02 instructs the operators to check and use operable instrumentation on SPDS, EFIC, and IDADS should NNI power not be available. The staff recognizes the benefit of using IDADS indication to monitor and confirm plant status, as it provides a multitude of plant process information to the operator. However, since the IDADS continues to receive some inputs from NNI-dependent instrumentation, the licensee must be cautious in allowing operator use of the system to achieve and maintain safe plant conditions for loss of NNI power events. Problems experienced during past ICS/NNI power failures have included the operators being misled by false/failed indications. The staff requested that the licensee discuss the precautions taken to ensure that operators will not be misled by false/invalid indications provided by the IDADS following ICS/NNI power losses. The licensee responded by stating that:

> Emergency operating procedures and the loss of ICS and NNI casualty procedures provide the operator with plant indications that are not affected by the loss, identifies indications that are affected, and provides alternate indications (which also include indication in IDADS) for the operator.

The staff believes that if the EOPs or casualty procedures continue to reference the use of IDADS displays for loss of ICS/NNI system power events, additional caution statements should be added to the procedures to warn the operators that IDADS displayed values other than those specifically identified in the procedure may be invalid and should not be used. In the staff's opinion, a better solution would be to either provide identification of IDADS displayed values dependent on NNI power (as was done for the SPDS and other control room indicators and recorders) so that the operators can recognize the dependency and avoid reliance on the associated indications, or, if possible, to avoid use of the IDADS displays for loss of ICS/NNI system power events. A review of Table 3.3 indicates that whenever the IDADS is listed as a backup source of information, other sources of information exist that are also independent of the ICS and NNI system.

It should be noted that steps 12.5 and 13.6 of procedure E.02 refer to the use of casualty procedures C.15, "Loss of NNI-X, Y and/or Z Power," and C.40, "Loss of ICS Power," respectively, after stable plant conditions have been obtained. These procedures specifically reference the use of instrumentation which will be independent of ICS/NNI system power. Refer to Section 3.1.2.10 of this report for the staff's evaluation of these procedures.

During the December 26, 1985 incident, the MFW flow recorders indicated near midscale because of the loss of ICS dc power even though MFW flow was actually zero. These recorders are located on the H1RI console (one for loop A flow and one for loop B flow). The recorders will continue to fail to the midscale position on loss of ICS dc power, however, because of the design change to trip the MFW pumps on loss of ICS dc power, failure to the midscale position should not adversely affect operator response. Also, as discussed above, the recorders will be fitted with color-coded labels to alert the operator of unreliable indication upon receipt of ICS or NNI system failure alarms. The EOPs will direct the operator to verify that the MFW pumps have tripped on loss of ICS power.

Conclusion

Considering the above evaluation, the staff concludes that the licensee has made significant design improvements to enhance the plant response to future loss of ICS/NNI system power events. In summary, the design changes include:

(1) automatic trip of the ICS ±24-V dc power supplies upon loss of NNI ac or dc power

(2) automatic trip of the MFW pump turbines upon loss of ICS power

(3) placement of the AFW flow control valves and ADVs solely under Class 1E EFIC system control

(4) the installation of MFW, AFW, ADV, and TBV isolation valves which will be operable from the control room independent of ICS/NNI system power

(5) the installation of controls to allow operation of the TBVs and auxiliary steam reducing station independent of ICS power

(6) the implementation of control room position indication for the TBVs, ADVs, AFW flow control valves, and MFW flow control and startup valves which will be powered independent of ICS/NNI system power

(7) the labeling of all ICS and NNI system hard-wired control room indicators and recorders

The staff concludes that the above design modifications will help ensure that the plant will be able to automatically or manually achieve a known safe state (as defined by the emergency operating procedures) following a loss of ICS or NNI system power. The staff further concludes that the modifications should significantly lessen the severity of loss of ICS/NNI system power events by preventing adverse equipment responses to ICS/NNI system power losses as have occurred in the past, and by preventing the loss of both automatic and remote manual control of key ICS-controlled equipment. The modifications should significantly reduce the burden on the control room operators by (1) allowing the operators to focus on a common plant response for all ICS/NNI system power failures through specific procedures on which they have been trained and (2) by positive identification of ICS/NNI system-dependent instrumentation, and the provision of adequate backup/alternate instrumentation, to achieve and maintain subsequent safe plant shutdown. On this basis, the staff concludes that the backup instrumentation for loss of control room controls is acceptable for plant restart.

3.1.2.8 Power Supply Monitor Design

This section discusses the purpose and application of the power supply monitor (PSM), describes the circuit design of the PSM, describes the role of the PSM in the December 26, 1985 loss of integrated control system (ICS) power and overcooling event at Rancho Seco, and discusses the results of the post-event onsite troubleshooting of the PSM performed by the licensee. The PSM-actuated shunt trip switches (S1 and S2), testing and analysis of the PSM by an independent laboratory, and corrective actions proposed by the licensee to improve performance of the PSM are also discussed.

As discussed in Section 3.1.2.2, "ICS/NNI dc Power Distribution System," one purpose of the PSM is to monitor the output of the +24-V dc and -24-V dc power supplies within the ICS and NNI system power distribution networks, and to activate ICS/NNI system trouble alarms in the control room if the output voltage of any of the power supplies drops to ±23.5-V dc. The alarms alert the operators to a loss of ICS/NNI system power source redundancy, and the need for maintenance/repair to restore redundancy, so that a subsequent failure does not initiate a loss of ICS/NNI system power transient. Another purpose of the PSM is to monitor ICS/NNI system ±24-V dc bus voltage, and to trip open switches S1 and S2 in the 120-V ac supply lines to both pairs of ±24-V dc power supplies (causing a loss of ±24-V dc power) and to activate ICS/NNI system failure alarms, if the voltage on either the +24-V dc bus or -24-V dc bus drops to 22.0 V dc. Thus, by design, the PSM transforms a loss of positive or negative bus voltage condition (a partial loss of voltage condition indicative of the loss of redundant power sources, and where ICS/NNI system modules are subject to malfunctioning in a manner that could cause erratic/unpredictable ICS behavior) into a complete loss of ±24-V dc power condition (a condition in which the ICS response is better defined and in which the plant operators can respond

to the loss by using specific procedures on which they have been trained). The ICS/NNI system PSM modules and PSM actuated shunt trip switches (S1 and S2) are housed in the ICS/NNI system instrument cabinets located just outside the primary operating area of the control room. The location of the ICS and NNI system cabinets is shown in Figure 3.25.

The basic building block of the PSM is an undervoltage detection circuit, such as is shown in Figure 3.26. As discussed in Section 3.1.2.2, each PSM consists of six undervoltage detection circuits. These circuits monitor the ±24-V dc power supply outputs and bus voltages, and provide outputs (relay contact closures) to actuate control room alarms and the S1/S2 shunt trip switches as discussed above. The circuit shown in Figure 3.26 is used to monitor voltage on the +24-V dc bus. The heart of each undervoltage detection circuit is an integrated circuit differential operational amplifier that compares its "variable" voltage input to its "reference" voltage input, and amplifies the difference between the inputs. The reference voltage is established by a constant voltage device called a zener diode. The variable voltage is determined from the PSM input/monitored voltage (V_{in}) as applied to a string of resistors arranged to form a voltage divider network. The variable resistor in the voltage divider network is adjusted so that the divided voltage input (variable input) to the operational amplifier will be less than the reference voltage when the monitored voltage is less than or equal to the predetermined setpoint values of 23.5 V dc (for control room alarms) and 22.0 V dc (for S1/S2 actuation).

When the monitored voltage is greater than the setpoint value (i.e., when the variable voltage is greater than the reference voltage), the operational amplifier drives itself into positive saturation and provides an output voltage (V_o) that approximates the supplied (input) voltage (V_{in}). In this case (i.e., when the monitored voltage is adequate/normal), the output voltage (V_o) exceeds the breakdown voltage of another zener diode and turns on the output relay driver transistor, thus maintaining the output relay in an energized state and illuminating the energized (untripped)/deenergized (tripped) status light on the front of the PSM module, signifying that the undervoltage detection circuit is in the untripped state.

When the monitored voltage is less than or equal to the setpoint value (i.e., when the variable voltage is less than the reference voltage), the operational amplifier drives itself into negative saturation and provides an output voltage of near zero volts. In this case (i.e., when an undervoltage condition is detected), the output voltage (V_o) is no longer sufficient to overcome the zener breakdown voltage, thus turning off the driver transistor and deenergizing the output relay and extinguishing the status light (signifying that the undervoltage detection circuit is in the tripped state). For the positive bus monitoring circuit shown in Figure 3.26, the tripping (deenergizing) of output relay K3 causes its associated contacts in the shunt trip coil circuits for S1 and S2 to close, thus energizing the shunt trip coils and tripping switches S1 and S2 to the open position.

There are some unique design characteristics of the PSM undervoltage detection circuits that should be noted. First, the voltage used to operate the detection

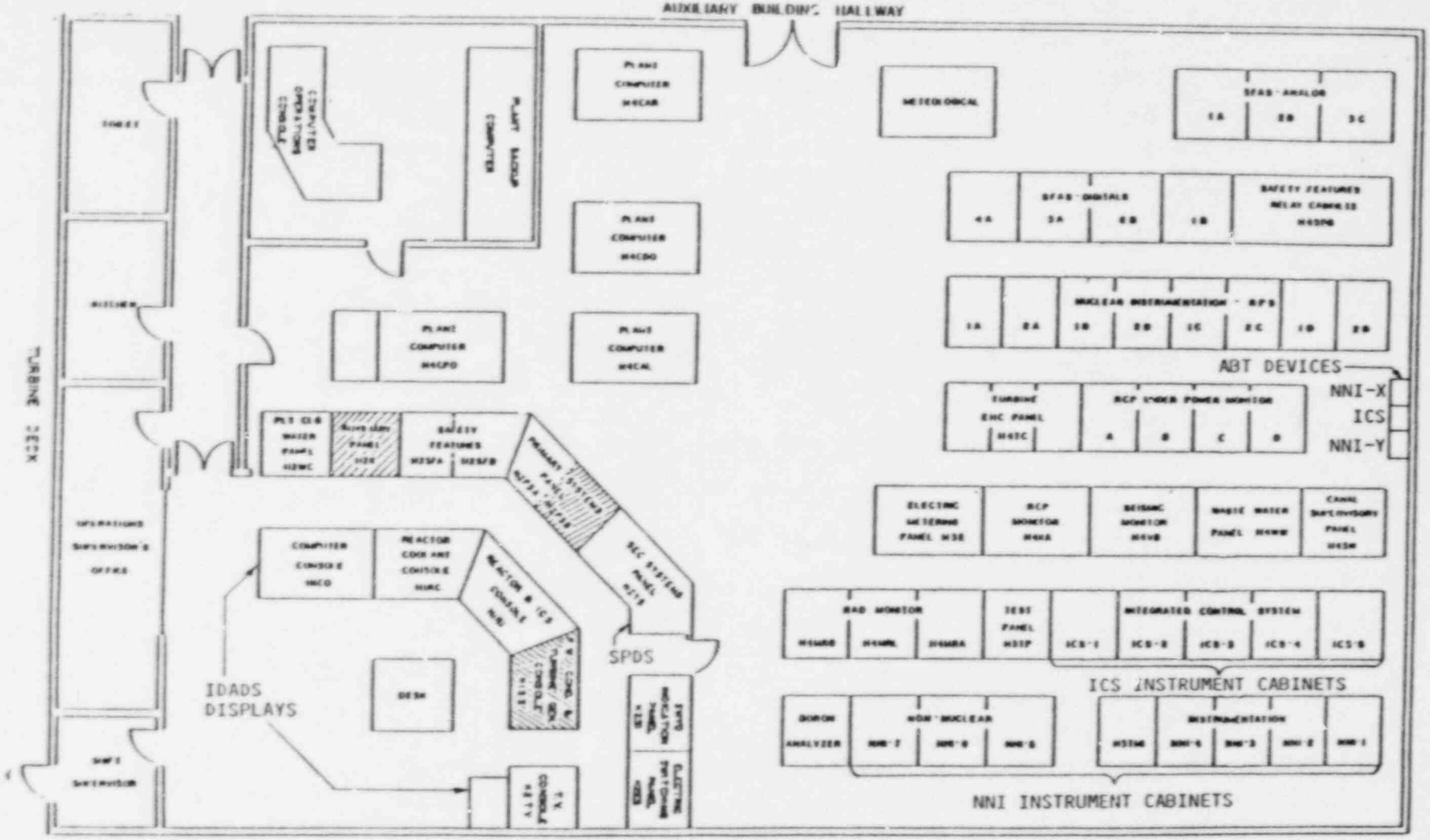


Figure 3.25 Control room layout

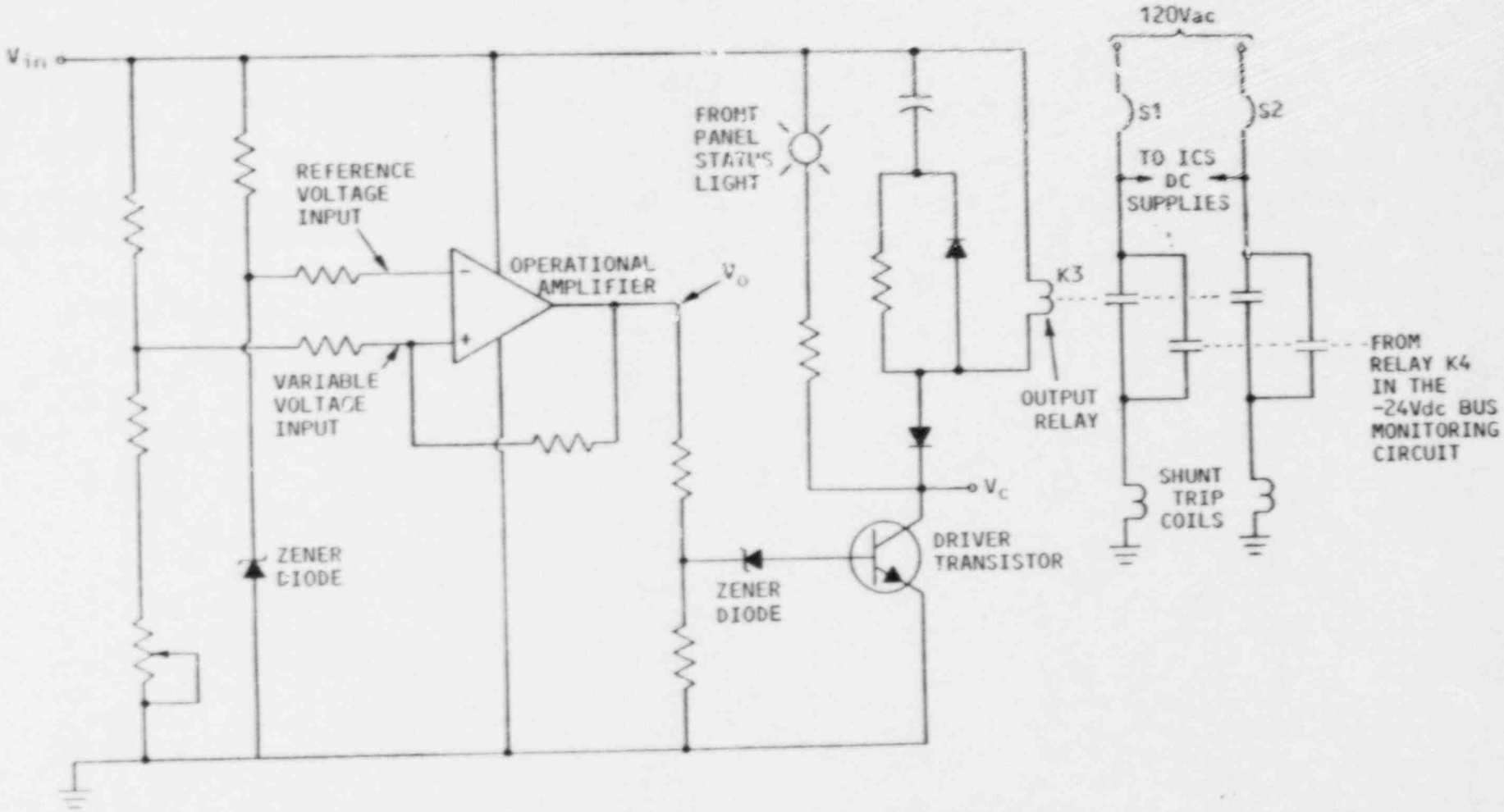


Figure 3.26 Power supply monitor, positive bus undervoltage detection circuit

circuits is the same voltage that is being monitored. A significant portion of the current required to operate each undervoltage detection circuit in the PSM module is that used to hold the output relay in its normally energized condition. Thus, the operating current of each detection circuit decreases when its output relay deenergizes (i.e., goes to the tripped state). Second, the circuit hysteresis (i.e., the difference between the operational amplifier negative saturation trip point and the positive saturation reset point) is designed to be very small (only 0.08 V dc). Third, the undervoltage detection circuits do not include any "seal-in" features (i.e., when the monitored voltage returns from below the setpoint value into the normal operating range, the output relays will automatically reset to the energized/untripped state). Additionally, it should be noted that the undervoltage detection circuit includes a capacitor that provides a 0.16-second time delay on dropout (trip) of the output relay after the drive transistor is turned off. The above design characteristics are significant with regard to understanding observed PSM behavior during the December 26, 1985 event and during post-event troubleshooting and subsequent testing of the PSM.

The shunt trip switches (S1 and S2) that operate to interrupt the ac input power to the redundant ±24-V dc power supplies are only actuated from one of two sources: (1) an automatic trip signal from the PSM, or (2) manual operation. Once S1 and S2 have tripped, they must be reset (closed) manually. The switch design includes a hydraulic time delay to delay opening of the switches upon receiving an automatic trip signal. The PSM vendor manual lists the delay time value as 0.5 second. The primary purpose of the time delay is to permit time for the output of the ±24-V dc power supplies to reach rated voltage upon energization without tripping S1 and S2. The time delay also helps to prevent spurious trips of S1 and S2 on short duration voltage fluctuations such as could be caused by switching transients.

Role of the Power Supply Monitor in the December 26, 1985 Event

The December 26, 1985 event at Rancho Seco was initiated by the loss of all ±24-V dc power within the ICS. The loss of power occurred when the ICS PSM signaled shunt trip switches S1 and S2 to open, causing deenergization of the ICS ±24-V dc power supplies. The ICS response to the loss of dc power initiated a plant transient as described in NUREG-1195, "Loss of Integrated Control System Power and Overcooling Transient at Rancho Seco on December 26, 1985." Twenty-six minutes after the loss of power occurred, an operator recognized that shunt trip switches S1 and S2 had tripped open, and restored power by reclosing the switches. The operators had inspected the ICS cabinets earlier, but failed to recognize that S1 and S2 had tripped.

The results of PSM testing (including testing of S1 and S2) to determine the reason for actuation during the event are discussed below. External factors that influenced the performance of the PSM as related to the root cause of the event are addressed in Section 3.1.2.1, "Root Cause of the December 26, 1985 Loss-of-ICS-Power Event," of the Rancho Seco Restart SER.

Licensee Testing of the Power Supply Monitor

In the first days following the event, the licensee developed a systematic troubleshooting plan to ascertain the root cause of the loss of ICS dc power.

Because the ICS shunt trip switches S1 and S2 had both tripped, and since the only automatic trip signal is provided by the PSM, it appeared that the most likely root cause was a malfunction of the PSM. The results of the licensee's in-place troubleshooting of the PSM include:

- The operation of the PSM +24-V dc bus undervoltage detection circuit was erratic. When bus voltage was reduced from 24 V dc to a value between 22.8 and 22.5 V dc, the output relay tripped and reset intermittently (the trip setpoint is 22.0 V dc).

- An abnormal voltage drop of approximately 1 V was measured between the positive bus and the input to the PSM, (V_{in}). The voltage drop was found to be due to a 2-ohm resistance created by a bad electrical connection in the distribution wiring between the +24-V dc bus and the PSM. When a jumper wire was used to connect the PSM input directly to the bus, the performance of the PSM improved, but was still not totally proper.

- The time delays of shunt trip switches S1 and S2 were measured to be 0.144 and 0.129 second, compared to the expected value of 0.5 second.

As part of the post-trip troubleshooting effort, strip chart recorders were installed to monitor the outputs of the ICS ±24-V dc power supplies. The licensee stated that the outputs were monitored for 34 consecutive days and no disturbances were recorded.

On the basis of the above test results, subsequent bench testing of the PSM, and a review of the PSM circuit design, it appeared that PSM operation was intrinsically sensitive to changes in voltage/resistance at its input. It appeared that this design characteristic of the PSM coupled with the resistance introduced at the PSM input because of the bad electrical connection, resulted in PSM actuation. The bad electrical connection is discussed in detail in Section 3.1.2.2.

Because an uncertainty existed about the specific root cause for the erratic behavior of the PSM observed during in-plant testing, the licensee agreed to send the ICS PSM and the associated shunt trip switches to an independent laboratory for circuit analysis, failure analysis, and testing.

Independent Laboratory Testing of the Power Supply Monitor

The original NRC agreement was that testing and analysis of the PSM by an independent laboratory would include (1) an analysis of the design of the PSM to determine the appropriateness of the design concept to serve its intended role and (2) an analysis of the details of the circuit design to determine the adequacy of the design to implement the design concepts. The licensee's direction to the independent laboratory, Science Applications International Corporation (SAIC), for testing of the PSM consisted of three required actions:

(1) investigation of PSM sensitivity to input resistance

(2) failure analysis of the PSM positive bus monitoring circuit

(3) failure analysis of the shunt trip switches

Although the scope of the independent laboratory testing did not fulfill the original NRC intent, the test results were beneficial in explaining certain PSM behavior observed during in-plant testing. The test results can be summarized as follows:

- A small resistance of a few ohms in series with the PSM input will cause changes in the setpoint, hysteresis, and switching characteristics of the internal comparator circuits.

- External series resistance alone was not found to be the cause of certain PSM behavior observed during in-plant testing, including oscillation, relay chatter, and failure to trip.

- A "cold solder joint" was found between the output lead of the positive bus monitor operational amplifier and the printed circuit board. The lead moved freely when touched with a probe and was withdrawn from the circuit board without having to reheat the solder. The cold-solder joint appeared to have been caused by poor workmanship when replacement the operational amplifier was replaced.

- A wide range of resistance (used in tests to simulate various degrees of a poor connection at the output of the operational amplifier) was found to cause relay chatter for input voltages near the setpoint, and could induce oscillations.

- The only apparent factor that could affect the delay times of the shunt trip switches as used at Rancho Seco was a change in the viscosity of the hydraulic damping fluid. The switch manufacturer guarantees the switch parameters for 5 years. The date codes on the S1 and S2 switches used in the Rancho Seco ICS indicated that they were almost 16 years old.

Considering the above findings, SAIC made three recommendations. The first two recommendations are:

(1) Implement a more rigorous procedure for printed circuit repair and rework including the use of a soldering standard and detailed inspection procedures.

(2) Replace the shunt trip switches S1 and S2 with equivalent switches that are less than 5 years old. The trip delay time should be verified at each refueling outage.

The staff interpreted the third recommendation as:

(3) Before any redesign or modification of the PSM, the PSM design should be reviewed and evaluated giving consideration to:

(a) different PSM circuit designs and voltage-sensing locations in the power distribution system

(b) the desired control system response to degraded power supply voltages to cabinets or groups of modules, such as could be caused by an external series resistance or open circuit in the power distribution system

SAIC concluded that system level reliability evaluations should be used to define any specific change (to the existing PSM configuration). The SAIC PSM test results are discussed in greater detail below. Modifications proposed by the licensee to improve PSM performance are also addressed.

Power Supply Monitor Sensitivity

The PSMs are intended to monitor voltage within the ICS/NNI ±24-V dc power distribution systems. The ICS PSM module installed at Rancho Seco received its input/monitored voltage via a series of connections associated with upstream modules. Except for a few thousandths of an ohm (milliohms) contributed by the intervening connections, there should be essentially no resistance present between the voltage being monitored and the PSM input. The existence of a series resistance as large as 1 ohm (such as could be introduced by a bad electrical connection) is extraordinarily high and indicative of a problem that needs to be corrected.

Before testing the PSM's sensitivity to input resistance, the as-found (as-shipped) trip setpoints and hysteresis values (i.e., the difference between the trip and reset voltages) were determined for each of the six undervoltage detection circuits. The as-found setpoints were all within 85 millivolts of the specified 23.5-V dc alarm and 22.0-V dc trip setpoint values, with the exception of the positive bus monitoring circuit setpoint which was 264 millivolts above the intended setpoint. The hysteresis values of all six undervoltage detection circuits were found to be close to the design value of 80 mV.

The PSM positive bus monitoring undervoltage detection circuit was tested for sensitivity to input resistance by applying an input voltage to the PSM that was slowly ramped down through the trip setpoint, causing a trip to occur, and then ramped back up until reset occurred (i.e., the input voltage followed a triangular waveform). This test was repeated for 13 different values of series input resistance, ranging from 0 to 55 ohms. For each test, the input voltage (V_{in}), the operational amplifier output voltage (V_o), and the relay driver transistor collector voltage (V_c) were recorded using an oscilloscope (refer to Figure 3.26 for the monitored voltage points). The expected voltages for a 0-ohm input resistance and the voltages observed for a 1.7-ohm input resistance are shown in Figures 3.27 and 3.28, respectively.

A series resistance at the input to the PSM would be expected to cause a voltage drop across the resistance, and hence a lower voltage being monitored/sensed by the undervoltage detection circuit than actually exists on the positive bus. Therefore, although bus voltage may be normal, the margin to the trip setpoint value decreases (in the direction toward PSM actuation), and the amount of the decrease would be expected to be essentially equal to the voltage drop (e.g., if the input resistance creates a voltage drop of 1 V so that the undervoltage detection circuit effectively believes that bus voltage is 23 V dc as opposed to an actual value of 24 V dc, then the margin to the

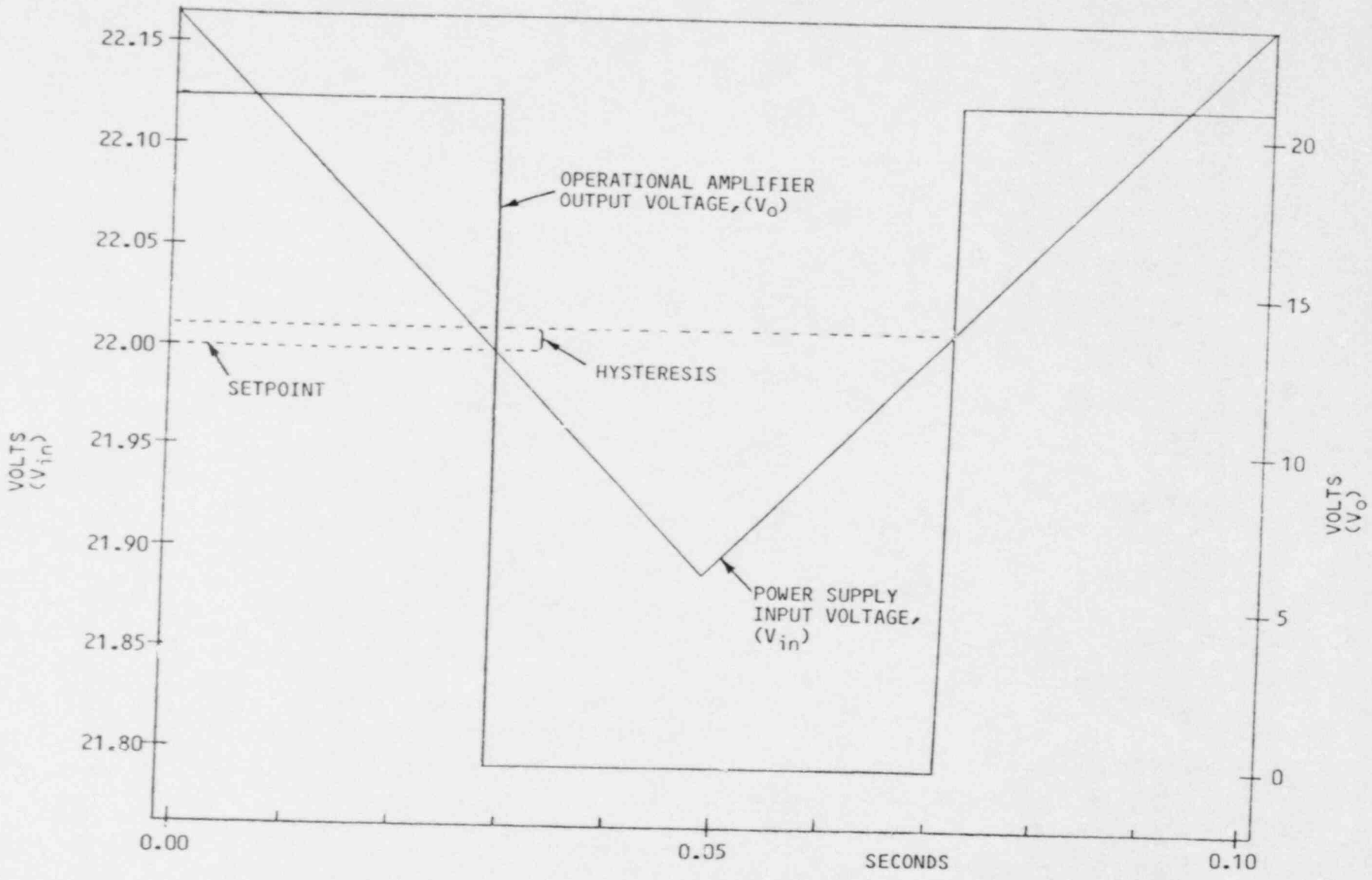


Figure 3.27 Power supply monitor, positive bus sensing circuit switching response with zero input resistance (ideal approximation)

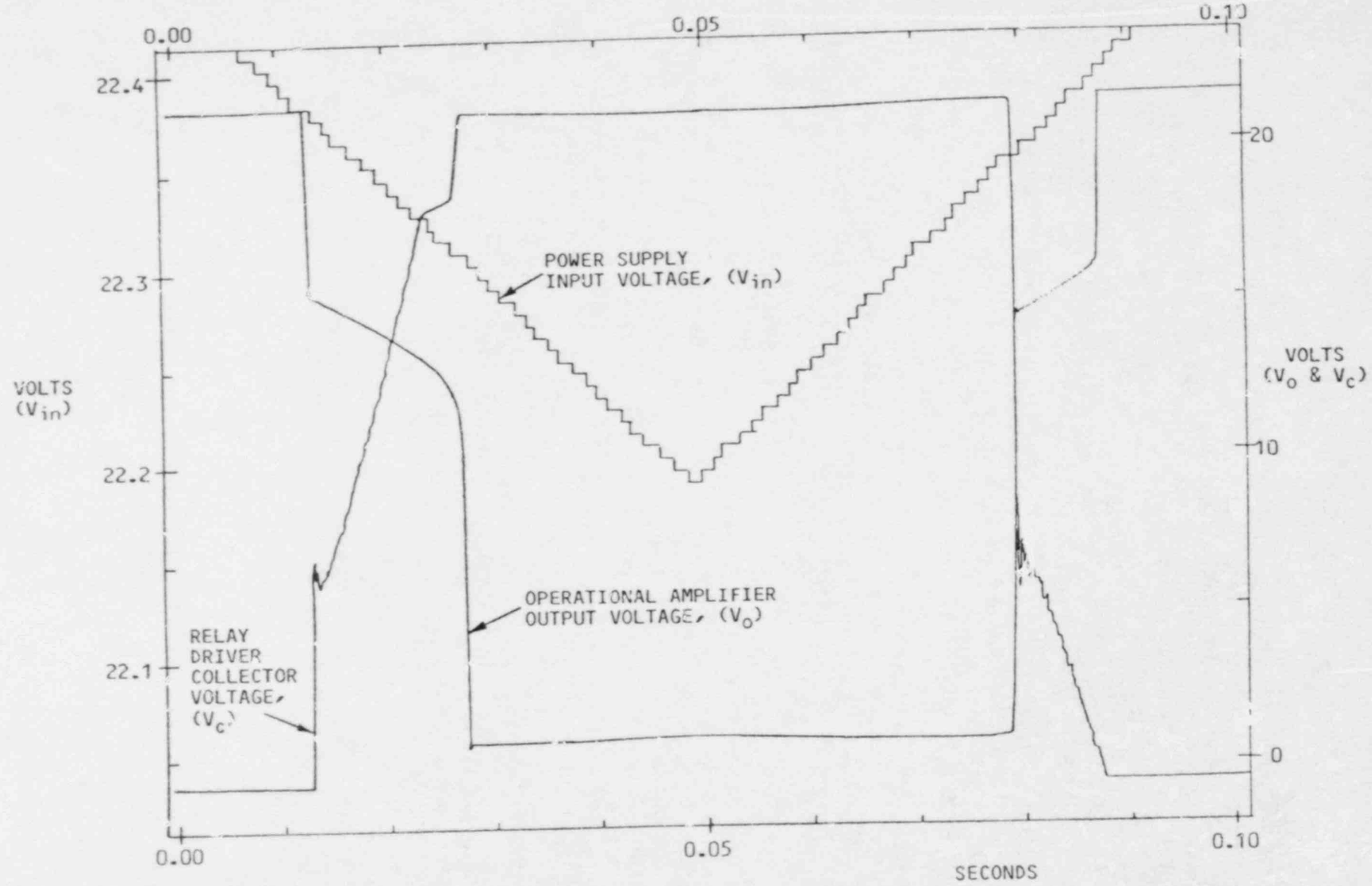


Figure 3.28 Power supply monitor, positive bus sensing circuit switching response with a 1.7-ohm input resistance

trip setpoint of 22.0 V dc would be reduced by approximately 1 V). However, since the operational amplifier comparator and output relay driver portions of the undervoltage detection circuit are also operating with a degraded voltage, the characteristics of the undervoltage detection circuit also change, causing it to behave in an abnormal manner. Instead of providing a sharp quick-action response upon the sensed input reaching the trip setpoint value (as shown in Figure 3.26), the circuit response becomes soft/slow and the trip setpoint value varies from its normal value as can be seen from Figure 3.28.

The as-found PSM setpoints indicate that a series input resistance was not present when the PSM was last calibrated before the event. The setpoint value for the positive bus monitor circuit was found to be off in the positive direction (i.e., higher than the desired value). If a series resistance had existed during calibration, the as-found setpoint for the positive bus undervoltage detection circuit would have been lower than the desired value to compensate for the voltage drop at the circuit's input (i.e., to provide sufficient margin to the setpoint value).

On the basis of the test results, SAIC concluded that the PSM was highly sensitive to input resistance, and that the PSM setpoints shift as a function of the voltage drops developed across the resistance (increasing the resistance effectively raises the setpoint). Additionally, the series resistance also interacts with the operational amplifier comparator and output relay driver circuits causing changes in the switching characteristics of these circuits.

The test data showed that with a 2-ohm resistance present at the PSM input (2 ohms was the resistance value introduced by the bad electrical connection as measured at Rancho Seco following the December 26, 1985 event), the trip setpoint changed by 0.08 V (from 22.01 to 22.09 V dc). The test data showed that with an input resistance of 10 ohms, the trip setpoint shifted upward by a value of only 0.34 V dc. The direct significance of a shift of this magnitude at first appears to be negligible. However, the current flowing through the resistor used to simulate the bad electrical connection during the test was only the current required by a single undervoltage detection circuit, and thus did not closely represent the current flow in the actual PSM application where a significant portion of the current flow through the resistance was that drawn by other ICS modules. The additional current flow would result in a larger voltage drop across the resistance. In addition, the input voltage was measured upstream of the series resistance during the tests. The actual voltage drop across the resistance was not recorded.

The value of the voltage drop across the series input resistance created by the bad connection is a key to assessing actual PSM behavior during the December 26, 1985 event. The PSM is located in ICS cabinet 2. The ICS ±24-V dc power supplies are located in cabinet 3. Power is routed to the PSM module in cabinet 2 from the ±24-V dc buses in cabinet 3 via cabinet 1. During in-plant testing following the event, the licensee used a jumper to connect the +24-V dc power feed in cabinet 2 directly to the +24-V dc bus, thus bypassing the distribution wiring in cabinet 1 where the bad electrical connection was found to be located. Upon installation of the jumper, the +24-V dc bus voltage provided to cabinet 2 rose by 0.5 V dc, thus indicating that the voltage drop across the resistance due to the bad connection was 0.5 V dc. Also, the resistance of the bad connection was measured and found to vary between 1 and 2 ohms. These two

bits of information indicate that the expected total current flow through the resistance created by the bad connection would be on the order of 250 to 500 mA. The licensee stated the current flow to ICS cabinet 2, as measured with a clamp-on ammeter during post-event troubleshooting, was found to be 400 mA, which is consistent with the expected values.

Considering the information available, it appears that the +24-V dc bus voltage sensed at the input of the undervoltage detection circuit must have been either (1) degraded by at least 2 V to reach the 22.0-V dc trip setpoint, or (2) degraded by 1.0 to 1.5 volts to reach the region where the PSM operates erratically.

The licensee asserts that at the time of the event, the resistance due to the bad connection had shifted from its post-event measured value of approximately 2 ohms to about 5 ohms, which caused a sufficient voltage drop to reach the PSM trip setpoint, causing PSM actuation of shunt trip switches S1 and S2, and that this deenergized the ±24-V dc power supplies to initiate the December 26, 1985 event. Although it is not possible to determine the exact characteristics of the PSM and its input circuit parameters that existed at the time of the event, the post-event troubleshooting which found that the resistance of the bad connection was varying (between 1.09 and 2.16 ohms) lends some credence to the possibility that the resistance could have reached a value as high as 5 ohms. There are a number of possible explanations for the cause of the increased voltage drop at the input to the PSM, including increased resistance because of changing mechanical characteristics of the bad connection or additional electrical current flow through the resistance due to control system switching (i.e., from the energizing of additional relays), or both.

The licensee's post-event investigations found that when the +24-V dc bus voltage was reduced to a value between 22.8 and 22.5 V dc, the undervoltage detection circuit output relay tripped and reset intermittently. The licensee's specification, "Testing Specification for the ICS Power Supply Monitor and the ICS Shunt Trip Switches," describes the erratic/oscillatory behavior in the following manner:

> With resistance in the line, the voltage in the PSM is lower than the bus voltage due to current draw from the circuit, in particular, the relay. As the resistance increases the voltage in the PSM decreases, approaching the setpoint. When the setpoint is reached, a transistor begins to turn off the relay, reducing the current drawn by the circuit and, therefore, increasing the voltage in the PSM. This causes the relay to be reenergized and in turn the voltage to drop again. This induces an oscillation which defeats the intended deadband of the circuit. The resultant dc voltage that the relay sees becomes dependent on the resistance, as well as the bus voltage.

The SAIC test report stated that no value of input resistance was found that by itself would reproduce the oscillatory behavior and relay chattering observed during post-event testing.

Considering the SAIC test results and the post-event troubleshooting performed by the licensee, the staff concludes that the voltage drop at the input of the PSM due to the resistance created by the bad electrical connection in ICS

cabinet 1 could have been of sufficient magnitude to cause erratic PSM operation and PSM trip of S1 and S2.

It should be noted that a poor solder connection at the output of the positive bus monitor operational amplifier (discussed below) existed during the SAIC input resistance sensitivity tests discussed above. These tests were rerun after the solder connection had been repaired and the test results, as far as PSM sensitivity to input resistance was concerned, did not change significantly.

Failure Analysis of the Power Supply Monitor Positive Bus Monitoring Circuit

During the in-plant troubleshooting following the event, the licensee discovered what appeared to be an intermittent internal failure in the PSM positive bus monitor circuit. On several occasions during the in-plant testing, and during subsequent bench testing without the presence of a series input resistance, the positive bus monitoring circuit would not trip at the 22.0-V dc setpoint, and did not trip until the input voltage was lowered to the point at which the output relay dropout voltage was reached. The licensee noted that though the series resistance problem showed up in all of the PSM undervoltage detection circuits, the intermittent internal failure only occurred in the positive bus monitor circuit. Additionally, as noted above, on other occasions when the +24-V dc bus voltage was reduced to test the positive bus monitor circuit trip setpoint, at input voltage values of between 22.8 and 22.5 V dc, the output relay was observed to chatter and oscillate between the energized and deenergized states.

Physical examination of the positive bus monitor circuit by SAIC revealed a "cold solder joint" at the output lead of the operational amplifier. The lead moved freely in relation to the circuit board and was withdrawn without having to heat the solder. Further examination of the PSM found that all operational amplifier circuits appeared to have been "replaced by hand," that substantial deposits of solder resin were located near the pins of some components (most likely due to heating to reflow the solder), and that some of the printed circuit foil pads had separated from the board. The results of the examination clearly point to a poor quality of workmanship relative to component replacement on the PSM printed circuit (PC) board. The B&W/Bailey technical manual for the PSM states that PC board repair should not be attempted in the field. The licensee has stated that there is no record of PSM soldering rework taking place at the Rancho Seco site.

After the December 26, 1985 event, the licensee purchased several PSM modules from another utility for use as spares. Each of the purchased modules was found to have similar poor soldering, suggesting that the poor soldering work may have been done by the vendor since the problem was common to both utilities. The licensee has informed the vendor of the results of the SAIC physical examination of the PSM.

The effects of resistance introduced at the output of the operational amplifier because of a poor connection from the cold solder joint were investigated by testing the module with different values of resistance between the operational amplifier output lead and its termination point on the PC board. The test results showed that: (1) the effect of resistance at this point in the undervoltage detection circuit on the trip setpoint value is in the opposite

direction to the effect caused by series resistance at the PSM input (i.e., resistance at the operational amplifier output causes a downward shift in the trip setpoint, in a direction opposite of that which would cause spurious trips); small resistance values caused the setpoint to shift only slightly downward (e.g., by 0.2 or 0.3 V), while very large values prevented the circuit from tripping until the monitored voltage dropped below the output relay minimum hold-in (dropout) voltage and (2) a wide range of resistance values caused relay chatter and circuit oscillations when the PSM input voltage was near the trip setpoint value, as was observed during the in-plant testing. The SAIC test report indicates that this erratic/oscillatory behavior becomes more pronounced when there is a series resistance present at the input of the PSM.

The "ICS OR FAN POWER FAILURE" alarm in the control room had intermittently actuated at least two different times in the weeks immediately preceding the event and three times after the event. The operators apparently considered the alarms that occurred before the event to be spurious. This alarm is actuated directly by contacts from the PSM output relays. The S1 and S2 switches remained closed at the time of the alarms. This suggests that if the decreased PSM input voltage due to the bad connection approached the trip setpoint value, the effects of resistance at the output of the positive bus monitor operational amplifier may be have caused chatter or oscillation of the output relay. Considering the results of the licensee's post-event troubleshooting and the subsequent testing by SAIC, both of which showed oscillatory behavior in the positive bus monitor circuit, it appears that the circuit may have tripped causing actuation of the control room alarm, but reset before it exceeded the combined delay times provided by the capacitor in the output relay circuit and the S1 and S2 switches, allowing the switches to remain closed. SAIC stated that the positive bus monitor as-found setpoint that was several hundred millivolts above the intended value (22.264 versus 22.0 V dc), and the absence of the circuit instability characteristics (found during post-event troubleshooting) upon receipt of the PSM for testing, indicates that a resistance was present at the operational amplifier output during the last PSM calibration preceding the event, and that the resistance had become small when received at SAIC, probably because the solder connection was disturbed during handling or shipping. The staff agrees with this observation which supports the assertion that a resistance existed at the output of the operational amplifier at the time of the event.

It is difficult to assess the impact of the cold-solder joint on PSM operation during the December 26, 1985 event. It appears that at the time of the event, the PSM exhibited characteristics attributable to both a series resistance at its input (i.e., an effectively increased trip setpoint and degraded undervoltage detection circuit switching characteristics) and resistance existing at the operational amplifier output (oscillatory circuit behavior and relay chatter at voltages that approach the trip setpoint). On the basis of the information available, it appears that the series resistance may have had the larger affect on PSM operation since the positive bus monitor circuit caused actuation of the S1 and S2 switches at input voltage values above the output relay dropout voltage. However, the affect of the cold-solder joint also appears to be significant as evidenced by control room alarms being received before the event without PSM actuation of S1 and S2.

The staff concludes that actuation of the ICS PSM during the event was not caused by a single factor, but was caused by a combination of the effects of a resistance in series with the PSM input (because of a bad connection within the +24-V dc distribution wiring to the PSM) and a resistance introduced at the output of the PSM positive bus monitor circuit operational amplifier (because a cold-solder joint caused a bad connection at this location). It appears that, in the absence of the series resistance at the PSM input, the oscillatory behavior of the circuit caused by the poor solder work may have never been detected through periodic surveillance testing. SAIC recommended that the switches be replaced with switches that are less than 5 years old, and that the trip time should be verified as between 0.2 and 0.8 second during each refueling outage.

Proposed Modifications to the Power Supply Monitor

The licensee has proposed no changes to the design of the PSM itself. The licensee has, however, changed the way in which the PSM is connected within the ICS and NNI ±24-V dc distribution systems. The change involves connecting the inputs of the PSM positive and negative 24-V dc bus monitoring circuits to termination points on the buses themselves, thus sensing bus voltage directly. The licensee believes that the PSM sensing location within ICS cabinet 2 at the time of the December 26, 1985 event, unnecessarily subjected the PSM to voltage drops at its sensing leads due to external resistances. The PSM was included in a "daisy chain" circuit that provides power to 23 additional ICS electronic modules. The staff agrees that changing the PSM sensing location directly to the ±24-V dc buses will help compensate for the disadvantage of having a PSM design that is susceptible to unstable/erratic operation given a resistance between the buses and the PSM input. The licensee has apparently not yet determined the optimum location for the PSM sensor.

One apparent advantage of locating the power supply module at the end of a daisy chain would be that the PSM would detect and provide protection for degraded voltage conditions within the distribution system (caused by individual module failures within the daisy chain) as well as for degraded voltage at the ±24-V dc buses. The staff acknowledges that in the existing ICS/NNI power distribution configurations which consist of multiple daisy chain end points, it is not possible to monitor the voltage to all system modules with a single PSM.

Ideally, it would seem that the PSM should trip (i.e., deenergization of the undervoltage detection circuit output relay to actuate S1 and S2, and appropriate control room alarms) the instant that the monitored/input voltage (V_{in}) decreases to the trip setpoint value, regardless of the reason for the voltage decrease or the rate of decrease. This would prevent the operation of ICS/NNI modules on unacceptable voltages outside of the ±24 V dc, ±10% range, specified by the module vendor. However, the B&W Owners Group (BWOG) now states that the design function of the PSM is to monitor the ±24-V dc power supply outputs to protect the ICS and NNI total systems against undervoltage caused by a hard short, and not to protect the system against all possible failures that can occur such as open circuits or increased resistance in the daisy chains. The staff believes that the PSM response to a hard short using a large instantaneous reduction in bus voltage as sensed at the PSM input would be acceptable regardless of the PSM location, even in the presence of a series input resistance and other PSM circuit malfunctions such as occurred during the December 26, 1985 event.

The licensee has stated that the BWOG has recommended modifying the PSM wiring in a similar manner to what was done at Rancho Seco (i.e., connecting the PSM inputs directly to the buses). In addition, during a telephone conference with the licensee on May 21, 1987, it was indicated that representatives of B&W stated that the sole purpose of the PSM is to detect faults on the buses and that the PSM should be connected directly to the bus. These statements, however, are somewhat inconsistent with (1) the procurement/design specifications for the ICS and NNI modules, that they will be supplied with 24 V dc ±10%, (2) the fact that some modules have malfunctioned when the voltage is degraded to only slightly below the -10% limit, and (3) the setpoint of 22.0 V dc which suggests voltage degradation protection rather than loss of bus or fault detection. In the staff's opinion, the PSM present design is not optimal for detecting degraded voltages in the ±10% range, as evidenced by the SAIC test results which showed PSM susceptibility to setpoint drift and erratic circuit switching characteristics at degraded input voltages within this range.

A voltage drop was created between the +24-V dc bus and the PSM (and other downstream modules) because a poor electrical connection existed during the December 26, 1985 event at Rancho Seco. There are a number of potential failure mechanisms that could cause degraded voltages of similar or greater magnitudes, resulting in module failures due to operation at unacceptable voltage levels. If the design function of the PSM is solely to detect hard shorts/bus faults, then a method should be provided to detect degraded voltages outside the ±24-V dc ±10% band. Operating experience has shown that although degraded voltage conditions do not occur as frequently as losses of voltage, degraded voltage conditions are not uncommon. Continuous on-line monitoring of voltage to all system modules using a device similar to a PSM, but one which is designed specifically for the function, would seem desirable. In the absence of continuous on-line monitoring, the daisy chain end points could be periodically checked to verify proper voltage. However, such testing has the drawbacks that (1) a degraded voltage condition may not be detected until some time after its onset (the absence of degraded voltage during testing does not ensure that the voltage will remain adequate during the interval until the next test) and (2) if permanent test jacks to allow easy connection of test equipment, or modifications to allow testing from the outside of the ICS/NNI system cabinets (e.g., multi-position test switches that connect the daisy chain ends to panel mounted voltmeters) are not provided, this testing might involve multiple temporary connections inside instrument cabinets, an operation which has been shown to be prone to human errors.

The licensee has tested all ICS and NNI system ±24-V dc power distribution daisy chain end points, and confirmed that the voltage provided to these points is adequate. This testing was performed as part of the licensee's program to verify the adequacy of electrical connections/terminations within the ICS/NNI system cabinets. However, the licensee currently has no plans to ensure that ICS/NNI system module voltage remains within the vendor specified ±24-V dc ±10% band. Potential voltage degradations that occur could go undetected. It should be noted that other periodic tests are planned for the ICS/NNI system, such as functional tests, calibrations, and system tuning, as discussed in Section 3.1.2.9 of this report, "ICS/NNI System Maintenance, Surveillance, and Testing." It is not evident that these tests would detect degraded voltage to an individual group or row of modules.

Consideration of Redundant Power Supply Monitors

The licensee's deterministic failure consequence analysis (DFCA) for the ICS/NNI power distribution system concluded that the effects of the plant response to loss of a 120-V ac bus were bounded by those associated with the loss of a 24-V dc bus. Because of the demonstrated ability of the loss of ICS/NNI system ±24-V dc power to initiate serious plant transients, and the application of the PSM module within the ICS/NNI power distribution systems that makes it a single failure point with regard to causing a loss of ±24-V dc power, the staff requested that the licensee investigate the desirability of using redundant PSMs arranged so that a loss of ±24-V dc power would be prevented upon failure of a single PSM.

The licensee conducted bench tests with three PSM modules connected in parallel to the same ±24-V dc power supplies. As the power supply voltage was reduced toward the trip setpoint value, the PSMs were observed to trip and reset with different variations until the supply voltage had reached the setpoint value at which time all three PSMs tripped and/or remained tripped. When the test was repeated with a small series resistance between the power supplies and the PSM inputs, the same interactions between PSMs were observed, the only difference being that the interactions started at higher voltage levels, as expected. The order in which the individual PSMs tripped and reset appeared to be strictly random. These tests demonstrate that the change in PSM load current due to its switching to and from the tripped/untripped states causes changes in the input voltage as sensed by the other PSMs, causing them to similarly cycle back and forth between the tripped and untripped states. The licensee has termed this behavior "cross-talk," and concluded that it could be a source of problems in using redundant PSMs. The staff concludes that the cross-talk observed is primarily the result of the lack of seal-in features within the PSM which allow it to automatically reset itself, and the extremely small PSM hystersis value of 80 mV. It may be appropriate to reconsider these PSM characteristics with regard to the test results.

The licensee has reported that PSM modules have had more than 150 plant-years of service without a failure. Furthermore, the licensee believes that the PSM did not fail during the December 26, 1985 event, but in fact performed its required function. This is contrary to the BWOG assertion that the sole purpose of the PSM is to detect hard shorts, which were not found to have existed during the event. The licensee's investigation into the root cause of the event states that "the design of the power supply monitoring system is such that it defeats the purpose of having redundant power supplies," and identifies this aspect of the design as a deficiency and weakness. However, the licensee has concluded that even though the PSM is a single failure point, the proven reliability of the PSM demonstrates that it is not a highly vulnerable failure point.

B&W performed an analysis to assess the impact of adding additional PSMs to the ICS/NNI system. The staff's interpretation of the analysis is that the benefit gained from adding redundant PSMs is a decrease in the frequency of ICS/NNI system power losses due to spurious PSM actuations. Since the rate of failure of the PSM to trip when required is thought to be small, B&W concluded that redundant PSMs will not significantly improve the reliability of the trip function. The analysis implies that the overall increase in ICS system reliability afforded by redundant PSMs is small, and that it is more important to

focus on reducing the consequences of ICS/NNI system power losses, which can still occur regardless of the number of PSMs installed. It is noted that the B&W PSM reliability assessment calculates that the spurious trip rate of the PSM would be improved from 8.7×10^{-3} to 1.2×10^{-6} through the use of redundant PSMs arranged in a two-out-of-three logic configuration. A reliability improvement of more than three orders of magnitude is likely to be significant. In view of the consequences of a spurious actuation of the PSM, the staff suspects that the cost/benefit ratio may be favorable toward the use of redundant PSMs.

Proposed Modifications to the Shunt Trip Switches

The licensee has stated that all S1 and S2 shunt trip switches installed within the ICS and NNI power distribution systems at plant restart will be less than 5 years old, and that all S1 and S2 switches will be replaced every 5 years in accordance with the manufacturer's recommendations to ensure that the delay times remain within the desired range (between 0.2 and 0.8 second).

In addition, lamacoid labels will be installed inside the ICS and NNI cabinets to provide the operators with a clearer indication of S1/S2 switch position. The labels will contain the wording "OPEN/TRIP" and "CLOSE" to accurately reflect the switch status. The labels use black letters on a white background and the letter size has been chosen for good visibility in accordance with accepted human factors practices.

Conclusions

The staff concludes that actuation of the ICS PSM on December 26, 1985 was most likely not caused by a single factor, but was caused by the combination of (1) an actual degraded voltage condition within the ICS power distribution system resulting from a poor electrical connection between the ICS positive 24-V dc bus and the PSM input and (2) a second poor electrical connection caused by a cold-solder joint in the PSM positive bus undervoltage detection circuit. The effects of the poor connections included PSM setpoint drift and unstable circuit operation, including relay chatter and oscillations.

The staff further concludes that the effects of the poor electrical connections were aggravated by questionable design characteristics of the PSM itself, specifically:

- use of the monitored voltage to operate the undervoltage detection circuits
- the lack of seal-in features upon sensing that the monitored voltage has exceeded alarm and trip setpoint values
- the small hysteresis value between the trip setpoint and reset point

It appears that PSM operation became erratic, during the event, when its input voltage decreased to a value between 23 and 22.5 V dc, which is between the normal operating value of 24 V dc and the trip setpoint value of 22.0 V dc. The erratic operation appears to have involved oscillation and relay chatter (cycling of the output relay between the energized and deenergized states).

Though the original design intent of the PSM is unclear, the staff concludes that (1) the existing PSM design is marginal in terms of ensuring that ICS/NNI system modules do not operate on degraded voltages outside of the vendor-specified ±24-V dc ±10% band where module performance has been shown to be unacceptable, and is not adequate for detecting degraded voltages due to resistance in series with the PSM input and (2) that although the PSM design appears to be better suited for providing detection of hard shorts/bus faults, that a means should be provided to ensure that ICS/NNI module operating voltage remains within the design tolerances specified by the vendor.

The licensee has modified the ICS/NNI power distribution systems by changing the PSM ±24-V dc operating/sensing input connections from points within the system module daisy chains to directly at the ±24-V dc buses themselves. This modification will reduce the probability of PSM malfunctions due to series resistance at their inputs. However, the staff is not convinced that the new PSM sensing location is as desirable as other possible locations.

The staff concludes that the new PSM sensing location selected by the licensee is acceptable for plant restart (following the December 26, 1985 event at Rancho Seco) on a temporary basis. The location is considered acceptable primarily because of other ICS/NNI system modifications designed to ensure that a known stable plant condition can be achieved following ICS/NNI system power losses (these modifications are described in Section 3.1.2.6 of this report, "Loss of Control Room Controls, Adequacy of Backup Instrumentation"), and secondarily because of inspections and tests conducted by the licensee to ensure that electrical connections within the ICS/NNI power distribution systems make good contact (thus eliminating series resistance problems at restart), and that the soldering rework of all installed PSMs is adequate. The staff finds that additional review is needed to determine what further changes should be made; this will be discussed in the staff's evaluation of the BWOG SPIP.

The staff agrees with the conclusion reached by an independent laboratory that the reduced delay time of the ICS S1 and S2 shunt trip switches was most likely due to deterioration of the switch's hydraulic damping fluid with age, and that the deterioration could have been detected by periodic surveillance, and could have been prevented by replacing the switches as the vendor recommended. The licensee has implemented preventive maintenance tasks for the Rancho Seco ICS and NNI system that include testing and verification of the shunt trip switch (S1 and S2) delay times at each refueling interval, and replacing the switches every 5 years as recommended by the vendor. The staff concludes that these actions are appropriate and should prevent reoccurrence of the switch delay times drifting beyond the design value.

The power supply monitor design is acceptable for plant restart, and the issue is closed as a restart issue.

3.1.2.9 ICS/NNI System Maintenance, Surveillance, and Testing

Description of Previous Program

The need to perform routine maintenance, surveillance and testing on integrated control system (ICS) and non-nuclear instrumentation (NNI) system components and actuated equipment to ensure and verify proper operation had been identified

before the December 26, 1985 Rancho Seco event as an important element necessary for improved ICS/NNI system performance. The BWOG identified poor maintenance and surveillance practices for ICS/NNI system components and equipment as a direct contributor to the frequency and severity of transients involving the ICS/NNI system at B&W plants. Inadequate maintenance, surveillance, and testing in general have been identified as contributors to events at plants of all designs.

At Rancho Seco, the preventive maintenance program as developed before the event was not well structured. Many of the maintenance manuals were controlled in an informal manner. This had been identified before the December 26, 1985 event, but the licensee had just started to implement the more important changes. The improvements that had been made apparently had no impact on the event. The ICS was not included in a functional surveillance program although tuning of the system had been improved before the event. Information from other plants and operational difficulties at Rancho Seco had not been adequately addressed and therefore problems reoccurred. For example, the existing ICS specification required that the ICS permit an instantaneous "bumpless" transfer from manual to automatic. This problem had resulted in previous plant trips that proper and complete testing would probably have identified. Circuit designs that would have permitted the smooth operation and would have met the specification were available but were not utilized. Previous (1982 and 1983) Davis-Besse Transient Assessment Program (TAP) reports revealed that the integral circuit for total feedwater flow control remained saturated after a rapid reduction in feedwater. Again, a complete testing program may have revealed this problem. The recommended installation of signal limiters was not applied to Rancho Seco. Following the "light bulb" event (March 20, 1978), Rancho Seco updated the NNI system power supplies and procedures but did not upgrade the ICS side. Following the January 5, 1979 loss-of-ICS event involving the loss of ICS power and reactor scram, Rancho Seco again did not upgrade the ICS power supply reliability or surveillance and testing procedures.

In [illegible], a fuse study was done for the NNI system at Rancho Seco. As a result of that study, all of the NNI system 5-amp fuses were replaced with 0.75-amp fuses. Nothing was done with the ICS at that time. When the ICS was recently reviewed (after December 26, 1985), it was determined that the ICS fuses also needed to be changed to 0.75 amp. There appeared to be a consistent failure to apply lessons learned to the ICS and NNI system and make corrections. ICS functional tests similar to tests already in place for NNI did not exist. Testing to verify operation on loss of ICS/NNI system power or the status upon repower also were not in place before the event.

Role in December 26, 1985 Event

The December 26, 1985 event demonstrated the previously identified need for adequate maintenance, surveillance, and testing. The lack of testing to determine the results of a loss of ICS/NNI system power was a major contributor to the December 26, 1985 event. As described in NUREG-1195, several items of concern were involved in this event.

- One of the two plant computers was out of service, reducing the data available to IDADS. Though not a safety-related system, the data are still useful in identifying problems and solving them.

- NUREG-1195 noted that the licensee had difficulty in identifying problems and solving them in a controlled, systematic, and well-documented manner, and noted that the licensee's usual maintenance practice was not well suited to the task.

- It appeared that previous damage to the AFW flow control valve B had not been corrected.

- The Velan instruction manual provided guidance for lubricating the manual AFW isolation valve (FWS-063); the guidance apparently was not followed.

During the licensee's investigation into the role of ICS equipment in the event, the ICS shunt trip switches S1 and S2 were found to have a time delay of 0.144 second and 0.129 second, respectively. The Bailey Controls Corporation technical manual states that this time delay should be 0.5 second. The manufacturer of the switches stated that the switches should operate with a delay between 0.2 and 0.8 second. The shorter time delay found makes the shunt trip more sensitive to short-duration transients that would not otherwise affect the ICS power supplies. These trip switches had not been included in surveillance before the event.

BWOG Recommendations

The licensee has reviewed the recommendations of the BWOG Instrumentation and Control (I&C) Committee, and is making the applicable specific changes in the Rancho Seco procedures. The licensee is also having its maintenance program certified by the INPO Good Practices Group. Many of the changes recommended by the BWOG and INPO are still being developed and will have to be evaluated by the licensee and the NRC before the proposed changes can be implemented. The BWOG reassessment report (BAW-1919) and the Rancho Seco restart situation have been reviewed concurrently. Some of the specific suggestions in the report are pertinent to Rancho Seco and are noted in this SER supplement. The staff will issue a separate safety evaluation on the BWOG reassessment. Revisions to the BWOG reassessment may result in changes or new requirements that pertain to Rancho Seco.

The importance of periodic ICS/NNI system preventive maintenance, surveillance, and testing was highlighted during recent events studied for the BWOG report (BAW-1919). Section IV, "Previously Identified Actions," lists "ICS Module Maintenance" as an area identified by the BWOG 1154 Task Force as requiring further attention by the BWOG. The 1154 Task Force was established to evaluate the consequences of the June 9, 1985 loss-of-feedwater event at Davis-Besse. The NRC staff report on this event is provided in NUREG-1154, "Loss of Main and Auxiliary Feedwater Event at Davis-Besse on June 9, 1985." The 1154 Task Force initiated action to determine if ICS maintenance procedures at B&W plants were adequate. Following the recommendation of the BWOG, Rancho Seco had initiated actions to upgrade its maintenance, surveillance, and testing activities in general, and for the ICS/NNI system in particular. The licensee did not have the programs completely in place by the time of the December 26, 1985 event. Several ICS/NNI system modules identified after the event were returned to the manufacturer (Bailey) for refurbishment and upgrading. The Davis-Besse ICS review had identified heat-damaged ICS modules; however, the potential for similar problems at Rancho Seco had not been evaluated before the event.

Following the Rancho Seco December 26, 1985 event, the BWOG recommended short-term action to all B&W facilities to "plan and initiate an evaluation of the ICS/NNI." The objective of the ICS/NNI system evaluation was to perform a comprehensive review of the ICS/NNI system to develop recommended improvements to limit the consequences of failures, and thus reduce the ICS/NNI system contribution to reactor trip frequency and complexity of transients. One of the major steps in the ICS/NNI system evaluation is to (based on detailed reviews concerning the ICS/NNI system) establish upgraded requirements for ICS/NNI system interfacing equipment and practices related to ICS/NNI system hardware design, and supplementary requirements for ICS/NNI system interfacing equipment and practices related to the ICS/NNI system, including maintenance, tuning, and operator training and qualifications.

A number of B&W plant transients and reactor trips have been attributed to improper maintenance and tuning of the components of the speed control system of the MFW pump included in or actuated by the ICS. An event involving a partial loss of NNI system power that occurred at Rancho Seco on March 19, 1984 was attributed to drift of the setpoint of an NNI-X +24-V dc power supply overvoltage protection "crowbar" circuit to the normal supply operating voltage, which tripped the "supply off" line. The redundant +24-V dc supply was not energized at the time; thus all of NNI-X +24-V dc power was lost. Investigation into the event revealed that the licensee did not perform periodic surveillance on the NNI power distribution system (e.g., power supply overvoltage trip setpoints, power supply monitor setpoints and delay times, ABT transfer and alarm setpoints, etc.). The staff asked the BWOG to address the ICS/NNI system power supplies' susceptibility to premature "crowbarring." This will be evaluated as part of the B&W reassessment review. It appears that implementation of a routine preventive maintenance and surveillance program for the ICS/NNI system at B&W plants will result in significant reduction in the frequency of reactor trips and the complexity of transients.

To improve reliability, the SAIC recommended monitoring the lower +24-V dc distribution buses for alarm conditions. This is currently under review by the BWOG. Appendix H of BAW-1919 provides the results of the BWOG 1154 Task Force review of the June 9, 1985 loss-of-feedwater transient at Davis-Besse. The objective of action item No. 13, "ICS Module Maintenance," of the BWOG 1154 Task Force Action Plan is to ensure that lessons learned from the Davis-Besse event are incorporated as applicable into the ICS preventive maintenance procedures at other B&W plants, including Rancho Seco. The examination of ICS equipment during investigations that followed the Davis-Besse event revealed that corrosion was found on at least one ICS control module (for the atmospheric vent valves), corroded switches were found that were difficult to operate, and excessive resistance existed across some switch contacts that were improperly tuned. An 1154 Task Force review of B&W plant preventive maintenance procedures for the ICS modules concluded that the types of problems concerning ICS maintenance found at Davis-Besse are common to all utilities and are typical of problems associated with other control systems. The 1154 Task Force review found that although all utilities had some program in place for periodic calibration of ICS modules, no utility had developed a proceduralized preventive maintenance program for ICS modules. The 1154 Task Force did not make any recommendations concerning ICS module maintenance since the I&C Committee is developing generic guidelines for ICS/NNI system preventive maintenance programs. The results

summary for action item No. 13 states that these programs should include procedures for cleaning switch contacts on ICS modules.

The objective of action item No. 14, "Reducing Feedwater Initiated Trips," of the BWOG 1154 Task Force Action Plan is to reduce the number of challenges to safety systems and increase B&W plant availability by focusing on the prevention of feedwater transients leading to reactor trips. The 1154 Task Force identified areas in which improvements in plant operations, maintenance, training, and equipment could potentially improve the performance and reliability of MFW systems. One of the 1154 Task Force recommendations concerning action item No. 14 is to "add to the current ICS preventive maintenance procedures a periodic check of all auxiliary relay contacts that are required to function during normal use." It is further stated that "as necessary, contacts with high resistance should be burned in to bring their resistance back within specification." The basis for these recommendations is that high-relay contact resistance can cause a significant plant upset when a relay changes position. The BWOG has stated that there have been "numerous incidents" in which high contact resistance initiated or contributed to a reactor trip. Another recommendation for action item No. 14 is to "add to the current ICS preventive maintenance procedures a post-refueling collection of baseline data from selected ICS modules to verify that the system is not deviating from previous steady state characteristics." It is further recommended that "an ICS tuning program should be implemented at each site." The basis for these recommendations is that the ICS needs to be dynamically tuned to ensure proper ICS operation. The inability of the plant to run smoothly at low and intermediate power levels with the ICS fully in the automatic mode is common. Interviews revealed that plant personnel held the general opinion that ICS operation was degrading. As a result, operators have frequently placed several ICS auto/manual stations in the manual mode during startup, and have generally accepted substandard operation of the system. The BWOG has stated that ICS and actuated equipment performance do differ with time. Feedwater pump governor linkages wear, control oil systems degrade, and valve stroke times change. The BWOG has stated that all of these factors decrease the effectiveness of the ICS to properly control the plant in a stable, predictable manner, and that dynamic tuning of the plant is the only way to verify that it will respond satisfactorily during startup and during transients. The BWOG has stated that the validity of the recommendation for dynamic tuning is confirmed by the operational difficulties being experienced at B&W reactors.

Section VI, "Operating Experience Review," of BAW-1919 describes the BWOG Safety and Performance Improvement Program (SPIP) review of the Transient Assessment Program (TAP) data base concerning events at B&W plants to identify areas for improvement. The initial review of the TAP data base focused on two areas: (1) transient initiators and (2) post-trip response. With regard to transient initiators, the BWOG developed a matrix of the causes (initiators) of reactor trips versus the reactor trip signals involved. The causes of reactor trips were divided into a number of categories (e.g., ICS module failures, ICS input signal failures, EHC system failures, main feedwater pump trips), including transients that were caused by human error during surveillance and testing activities. These data show that out of the 212 category A, B, and C events involving a reactor trip at B&W plants between 1980 and 1985, 11 of these events were initiated by human error during surveillance and testing activities. Another 24 events were initiated by human error while personnel were performing maintenance on plant equipment. The data do not indicate the number of

events caused by maintenance, surveillance, and testing activities involving the ICS/NNI system versus other plant equipment (e.g., the main turbine, feedwater system pumps and valves, reactor coolant pumps, control rod drives).

The data provided in Section VI of BAW-1919 show that the number of trips related to surveillance and testing is less than 20% of the total number of trips related to human error. Furthermore, the number of trips related to surveillance and testing is less than 1% of the total number of reactor trips attributable to all causes. Based on (1) the demonstrated need for ICS/NNI system preventive maintenance and surveillance for improved system performance and reduced ICS/NNI system contribution to reactor trips and complexity of transients and (2) the small contribution of human error during surveillance and testing activities to the frequency of reactor trips, the staff concludes that the benefits gained from ICS/NNI system surveillance and testing (e.g., more rapid detection of failed/degraded components, more stable plant operation, verification of system operability, decreased contribution to reactor trips and complexity of transients) far outweigh any potential disadvantage (e.g., possible inadvertent reactor trips attributable to human error). The staff notes that improved and carefully developed maintenance and surveillance procedures could be expected to further reduce the number of trips resulting from human error. The BWOG has indicated that most ICS/NNI system maintenance activities will be performed during periods of plant shutdown or during power escalation following reactor shutdowns/refuelings, thus minimizing the potential for, and consequences of, inadvertent reactor trips during ICS/NNI system maintenance.

The BAW-1919 document also reported on interviews with operator/maintenance personnel and on "brainstorming" sessions. These interviews noted that (1) a greater effort is required to reduce the backlog of recommendations and work orders, (2) generic procedures should be developed and records should be established to verify that non-safety equipment is being maintained, and (3) after refueling, baseline data should be collected from selected ICS modules to verify that the system is not deviating from previous steady-state characteristics.

Appendix R of BAW-1919 ("ICS/NNI Evaluation Final Report") entailed a 1-year investigation by the BWOG I&C Committee. Some of the level 1 recommendations for immediate improvements include:

- surveillance testing of the automatic bus transfer
- periodic surveillance of ICS and NNI system cabinet dc voltage
- periodically record ICS module input and output voltage
- periodically test functions of ICS not normally demanded
- periodic full load test be performed for each dc power supply (test to be performed when plant is not operating)

The level 2 and level 3 recommendations involve long-term major system changes and the installation of the new digital advanced control system to replace the ICS. These items are not currently scheduled for implementation at any plant in the near future.

The ICS/NNI and Related Equipment Preventive Maintenance Program developed by the BWOG I&C Committee includes the following maintenance, surveillance, and testing activities:

- Clean, inspect, and calibrate all NNI-X and NNI-Y modules.
- Test the NNI-X and NNI-Y instrument channels, including indications, alarms, and recorders.
- Clean, inspect, and calibrate all ICS modules, ac and dc relays.
- Functionally test the ICS subsystem (i.e., unit load demand, integrated master, feedwater demand, and reactor demand) control functions.
- Calibrate and stroke time test the feedwater control valves and turbine bypass control valves from the E/P(I/P) converter through the valve position.
- Calibrate the feed pump turbine governor control system and inspect any mechanical linkage.
- Check the applicable dc power supply trip setpoints, power supply monitor, and S1 and S2 delay times, and inspect and check ac and dc power supply wiring for good continuity and connections.
- Record and/or verify ICS and NNI system setpoint settings, including bias settings, and compare against previous settings from module records and resolve differences.
- Dynamically tune the ΔT_c controller and turbine bypass valve controllers.
- Dynamically tune the T_{ave} control of feedwater.
- Dynamically tune the turbine header pressure control loop on turbine demand, and the normal T_{ave} control on rod control demand.
- Monitor selected control signal voltages within the ICS and/or NNI system at approximately 10%, 40%, 60%, 80%, and maximum obtainable power.

The NRC staff notes that although this program does not include them, the upstream power train components must also be included in the periodic maintenance and surveillance.

The ICS tuning guideline has been issued in the final revision of BAW-1919. It is expected that B&W will suggest that the individual plants follow this outline. The purpose of this test is to provide a method for adjusting the ICS during steady-state, transient conditions and in the following modes of operation:

- integrated reactor/steam generator/turbine
- reactor/steam generator following
- turbine following
- turbine and feedwater control following the reactor

The B&W ICS/NNI and Related Equipment Preventive Maintenance Program essentially calls for half of the above maintenance, surveillance, and testing activities to be performed during each refueling outage and/or at power escalation. The

maintenance, surveillance, and testing not performed at a given outage would be performed at the next outage so that all specified ICS/NNI system maintenance and surveillance would be performed at least once every two operating cycles. No justification was provided for these intervals.

The BWOG I&C Committee has prepared an "ICS/NNI Evaluation Matrix" which is intended to coordinate the ICS/NNI system design requirements and the associated design-basis and acceptance criteria, and give the status of individual B&W plants with regard to compliance with the requirements. The ICS/NNI system evaluation matrix states, as part of the ICS/NNI system design basis, that a preventive maintenance program is required to ensure long-term, day-to-day operation of the systems. The associated acceptance criterion is that a documented preventive maintenance program for the ICS/NNI system must address instrumentation string testing, calibration and maintenance of modules and actuated equipment. The ICS/NNI system evaluation matrix design basis also states that proper system control is dependent on correct adjustments of control loop gains to account for desired performance and actuated equipment response. The associated acceptance criterion is that plant control should respond to system inputs without instability and with proper responses to avoid initiation of upsets or transients. The ICS/NNI system evaluation matrix design basis further states that on-line data collection to predict and/or discover potential component failures or poor performance before ICS operations can reduce challenges to safety systems. The associated acceptance criterion states that means shall be available at each site to collect on-line data of plant parameters and critical control signals to monitor control system performance.

The ICS/NNI system evaluation matrix indicates that, in general, B&W plant-specific designs do not satisfy the above design-basis and acceptance criteria concerning ICS/NNI system maintenance, surveillance, and testing. The BWOG has recommended that utilities should upgrade the capability for data acquisition for on-line monitoring, that preventive maintenance programs need to be developed, and that system or sub-system tuning should be performed by plant procedures in accordance with vendor recommendations, or at least at every other refueling outage. It is not clear to the staff that a surveillance frequency of "at least every other refueling outage" is adequate to fulfill the intent of the original BWOG recommendation to require periodic ICS/NNI system surveillance/preventive maintenance (i.e., to improve ICS/NNI system reliability, thus reducing their contribution to the frequency of reactor trips and complexity of transients). Loss-of-ICS/NNI-power events at B&W plants have been attributed to the lack of preventive maintenance and/or surveillance. The staff considers that electrical/electronic equipment should be checked for operability/drift yearly if not more frequently, depending on its application, environment, and the consequences of failure. The BWOG should provide information in the ICS/NNI system design-basis documents that demonstrates the acceptability of the frequencies selected for periodic surveillance and preventive maintenance.

The maintenance, surveillance, and testing functions specified in the BWOG ICS/NNI system requirements, the ICS/NNI and Related Equipment Preventive Maintenance Program, and the ICS/NNI system evaluation matrix documents use somewhat general/vague language, and may not provide sufficient guidance for individual utilities to develop an adequate maintenance and surveillance program. The BWOG should revise the documents to specify the individual maintenance and surveillance actions considered necessary to ensure proper operation of the

ICS/NNI system and actuated equipment (e.g., explicitly define the scope and intent of instrument string tests and calibrations, identify the power monitor alarm and trip setpoints to be tested and their recommended values, specify the control signals to be monitored during power escalation after an outage, and identify for plant personnel problem areas/symptoms to watch for, etc.). In addition, the ICS/NNI system and Related Equipment Preventive Maintenance Program should be revised to include periodic checks of auxiliary relay contacts, and requirements to burn in contacts with high resistance, as recommended by the BWOG in recommendation No. 4 of action item No. 14 of Appendix H of BAW-1919. The staff believes that detailed guidance should be provided to the individual owners of B&W reactors to allow an understanding of the rationale for the recommended maintenance and surveillance activities, and to ensure that the desired increase in ICS/NNI system reliability and a reduction in the frequency of reactor trips and complexity of transients is attained through the maintenance and surveillance program.

Rancho Seco Program Modifications

(1) Preventive Maintenance

At Rancho Seco, the preventive maintenance (PM) tasks are tracked together with those preventive maintenance tasks that generate specific work requests. The tasks themselves are used to generate the specific work request and the frequencies with which the PM will be performed. When the work request is issued, the references and any detailed instructions are included along with the administrative information. In a typical work request, one of the references will be the vendor manual. The staff notes that the vendor manuals usually provide adequate calibration information but, in general, do not provide repair guidance. A typical manual directs the user to replace the component with a known good component and ship the malfunctioning unit back to the manufacturer. The PM manuals at Rancho Seco are now controlled documents; the NRC staff believes this will help ensure accuracy. Currently, the procedures indicate that one-half of the ICS modules will be calibrated and cleaned each refueling outage, and the ICS functional testing and tuning will be performed at each refueling. This is consistent with recommendation 14 of the System Status Report. The NNI system modules will be cleaned and calibrated each refueling outage. The S1 and S2 switches shall be replaced every 5 years. ICS cabinets 2 and 3 will be calibrated during the first refueling under task No. PM05746; cabinets 4 and 5 will be calibrated under task No. PM05745. All panels will be recalibrated for this restart.

According to the ICS System Status Report (Revision 1), cleaning and inspection maintenance performed after the event on the ICS bias circuit boards revealed discoloring due to heat similar to that previously (before December 26, 1985) noted at Davis-Besse. The licensee's discussions with representatives of the Bailey Controls Corporation revealed the availability of a modification of the bias circuit board to eliminate the problem, and the modules have been returned to Bailey to incorporate the upgrade. Other B&W-recommended module upgrades have been incorporated.

(2) Integrated Loss-of-ICS/NNI-System-Power Test

STP.664 (Revision 1, February 10, 1987) is a one-time loss-of-NNI/ICS-power test which is intended to verify that the plant reacts correctly and goes to a known

safe condition. The licensee may choose to perform this test for more than one shift to provide additional training to operators. The NRC staff believes that because of past problems, this test should be performed or monitored by all operators.

The objective of the test is to demonstrate that the plant can be brought to and controlled in a hot shutdown condition following loss of ICS/NNI system power. The test will require changing to applicable casualty and annunciator procedures as well as module calibration and EFIC testing. Following this test, the licensee will check the data collected to verify compliance with the following acceptance criteria:

- ICS power trips on the loss of NNI system power. Tripping the ICS on loss of the NNI system is a short-term solution. The long-term solution will be provided by the recommendations of an analysis to be completed by the licensee's nuclear engineering group. That analysis is not expected before restart.

- The main feed pumps trip on the loss of ICS power.

- Pressure control of auxiliary steam is not lost on a loss of ICS power.

- The TBVs are controllable by operators in the control room on a loss of ICS power.

- No SPDS parameters necessary to bring the plant from power operation to hot shutdown are affected by the loss of NNI system power.

- The multipoint recorder (UJR-10104), which provides indications of actions necessary to bring the plant to hot shutdown without the NNI system, is not affected.

- The analogue indications on the boron analyzer/shutdown panel are not affected.

- The labeling of the ICS and NNI system-related indicators in the control room distinguishes the affected equipment during a loss of ICS/NNI.

- There should be no problems with annunciator procedures (H2PSA and H2PSB) related to the ICS power loss.

- The ICS memory modules repower to their predetermined states. To facilitate this, the licensee is replacing all memory modules with modules that can be preset to a specific repower state.

- NNI system channels are not affected by the loss of ICS power.

The staff considers this test to be a valuable demonstration of the plant's capabilities to reach a hot shutdown after the loss of ICS/NNI system power. It should be noted that since this test is started from a hot shutdown status, the reactor trip functions are not tested. Past operations have adequately demonstrated this trip function. Testing in accordance with STP.664 should provide an improvement in plant response to the loss-of-ICS/NNI-system power

transient and should provide a marked improvement in overall plant safety. One item in the procedure should be changed before the test is performed. Steps 4.4 (NNI-X) and 4.8 (NNI-Y, Z) are the steps that trip the ICS power, no step was included that trips the ICS power while the NNI system is not tripped. Step 2.12 of the acceptance criteria states that it must be shown that NNI system channels are not affected by the loss of ICS power.

The licensee has stated that the test procedure is being revised to include a step to verify that there is no detrimental loading effect of the ICS on the NNI system when ICS power is lost. The affected ICS modules have been modified to preclude NNI system signal loading. This is acceptable to the staff.

(3) ICS Functional Test

This specific test (STP.778, Revision 1, September 8, 1987) is intended as a one-time pre-restart test. The intention, as explained by the licensee's staff, is to use this new test as the basis for a surveillance test to be performed every refueling outage. The only change that has been identified to date to change the one-time test to a regular surveillance test is the removal of Section 6.8, "Boundary Test." It is expected that once the boundary conditions are established there will be no changes without a significant change in plant configuration; this would require a complete reevaluation of the procedure.

The test objective will be to demonstrate that the ICS can perform the functions necessary to control the reactor, the once-through steam generators, and the turbine over the plant's full range of power by using simulated inputs to the ICS and observing the system's reaction. The simulated inputs will be provided by a portable test fixture. The test is designed to verify each wire and device in the ICS cabinets. The licensee noted that B&W had reviewed this test independently. The staff has reviewed Revision 1 of STP.778 submitted in the licensee's letter of October 12, 1987, which declares that Revision 1 is a final product.

Prerequisites for the test include module calibration and pretest briefing of the test participants. This test will be performed only at cold shutdown. Independent verification will be required to ensure the plant is in manual operation before the test is initiated.

Throughout the test, the following alarms will be annunciated:

- H2PSA-57, ENABLE BORATE/DEBORATE
- H2PSB-1, ICS RUNBACK OR LIMIT
- H2PSB-24, SGA ON LO LVL LIMIT
- H2PSB-25, SGB ON LO LVL LIMIT
- H2PSB-34, ICS TROUBLE
- H2PSB-35, SGA ON BTU LIMIT
- H2PSB-36, SGB ON BTU LIMIT
- H2PSB-64, ICS SYSTEM FAILURE

The following testing guidelines have been recommended in the ICS System Status Report.

The ICS unit loading demand subsystem will be tested to verify:

- manual operation
- tracking operation
- runbacks
- load change rates
- load demand limit

The ICS integrating master subsystem will be tested to verify that it:

- transfers turbine controls to manual on a large steam header pressure error
- provides manual/automatic controls for the steam generator/reactor demand and turbine bypass valves
- changes steam header pressure setpoint on turbine operation or a reactor trip
- opens TBVs on high steam generator pressure
- closes TBVs on loss of condenser availability

The ICS reactor control subsystem testing will check:

- auto/manual control for reactor demands
- reactor control limits
- cross-limits
- neutron power blockage of restart of reactor coolant pumps
- neutron error blockage of transfer of rod control to automatic
- asymmetric rod condition blockage of rod withdrawal

The steam generator/feedwater subsystem will test the:

- manual/automatic controls for feedwater demand, feedwater pump speed, feedwater valve position and ΔT_c
- steam generator BTU limits
- minimum and maximum steam generator level
- cross-limit
- re-ratio feedwater on loss of reactor coolant pumps

The borate control subsystem will be tested to verify annunciation or rod position error and operation of the feed-and-bleed permissive.

The System Status Report for the ICS notes that the testing is planned for every refueling outage. The staff considers this a reasonable schedule. The current suggested schedule of every third refueling for calibration is considered by the staff to be less than optimal unless a basis is established for such calibration intervals.

(4) NNI System Functional Test

This test differs from the ICS functional test in that it serves more as a checklist of separate surveillance procedures and preventive maintenance procedures, but the ICS test is more of a stand-alone document. The NNI system functional test STP.1115 reviewed by the staff was the September 28, 1987 (Revision 0) version that the licensee submitted on October 12, 1987 as a final version.

The test objective is to verify that the NNI system functional testing has been performed as part of the restart program. In addition to the instrumentation calibration maintenance, the power supplies, power supply monitors, shunt trip switches, and ABT switch maintenance procedures will be performed. Each specific item required is listed for each part of the functional test. For example, this procedure includes a step to verify that preventive maintenance task 05390 for the NNI system shunt trip switch S2 has been performed. This test will be performed at each refueling outage. Some NNI system testing and calibration had been performed before the December 26, 1985 event. These tests and procedures have been added to, revised, formalized and, in the staff's opinion, improved. Procedure I.40, "Functional Testing of the Signal Conversion Cabinets," contained several errors; these errors were corrected in Revision 1, dated March 30, 1987.

(5) ICS Tuning at Power

The ICS tuning-at-power procedure, STP.660, will verify that the ICS provides the optimum load response to the unit load demand during steady-state and transient conditions. This is accomplished by inducing transients, adjusting tuning parameters, observing power escalation, and verifying the calibration of the feed forward function generators. The staff reviewed Revision 1, dated October 14, 1987, which was provided by letter dated November 5, 1987; this letter noted that no further submittals are scheduled. This procedure is based on the recommendation of the BAW-1919 guidelines and has been reviewed by B&W representatives.

Before this test is performed, the ICS functional test and instrument calibrations must be completed. This test will be conducted by a "tuning team" which will consist of, at a minimum, a level 3 test engineer, a senior control room operator, and a journeyman technician, all who have experience and training in the ICS. This test will be run at power levels that range from startup to full power.

The following parameters will be tuned:

- steam generator startup level
- turbine bypass control
- feedpump time response
- automatic level/flow control
- low feedpump ΔP control
- flow control (one pump)
- reactor power control (low power)
- T_{ave} control (low power)
- turbine header pressure control (low power)

- feedpump controller
- flow control (two pumps)
- ΔT_c control of feedwater (medium power)
- T_{ave} control (medium)
- T_{ave} control by feedwater (medium power)
- turbine header pressure control (medium power)
- flow control (full power)
- reactor power control (full power)
- ΔT_c control of feedwater (full power)
- T_{ave} control (full power)
- T_{ave} control by feedwater (full power)
- turbine header pressure control (full power)
- turbine following mode control (full power)
- steam generator/reactor following control (full power)
- unit load transient (maximum thermal)
- function generator curve verification (various power levels)
- unit load transient (maximum thermal)
- function generator curve verification (various power levels)

This procedure should provide a significant improvement in the overall plant performance and may allow the operators to spend less time compensating for imprecise ICS control.

(6) Operational Surveillance

AP.23.03, "Logs of Rounds" (Revision 0, March 6, 1987), will be used to establish logs and rounds sheets for identifying abnormal conditions and operating history, and for transferring information between shifts and providing guidance to operators on the methods used to take readings, identify abnormal readings, and to take corrective action.

As shown by the references in AP.23.03, this procedure is derived mainly from INPO Guidelines and Good Practices. As noted before, Rancho Seco is having its maintenance program accredited by INPO. The rounds are scheduled to be done at the beginning and middle of each shift; the first check will be a verification of the operating parameters and the second (shorter) check will verify function. In addition to the control room equipment status indications, the control room instrumentation and indication round also checks the ICS/NNI system cabinets to verify that the power and trip logic operable lights are on. The required technical specification checks and other important instrumentation checks are done under surveillance procedures (SPs). SP.200.01, "Instrumentation Surveillance Performed Each Shift" (Revision 32, March 13, 1987), checks the technical specification requirements such as the core power imbalance calculations performed every 2 hours. Guidance on methods and a table for entering the data are provided directly on the procedure. SP.200.02, "Instrumentation Surveillance Performed Each Day" (Revision 21, March 20, 1987), references the specific technical specification that it addresses and provides similar checklists. SP.200.03 (Revision 13, April 28, 1986), is the weekly instrumentation surveillance procedure. Although not a specific check on ICS/NNI system functionality, the various surveillance procedures check some of the parameters

that are controlled by ICS. The operator may check ICS/NNI system instrumentation, in addition to the Class 1E equipment, during the surveillance.

Summary of Evaluation

On the basis of the review of information provided in BAW-1919, the staff concludes that, in general, BWOG is appropriately emphasizing the need for upgraded maintenance and surveillance programs for the ICS/NNI system, and recognizes the associated potential benefits of improved ICS/NNI system performance and a decrease in the ICS/NNI system contribution to reactor trip frequency and the complexity of transients.

It also appears that Rancho Seco, in particular, has started to place proper emphasis on the need to establish maintenance, surveillance, and testing for ICS/NNI system components and actuated equipment. The staff considers proper maintenance, surveillance, and testing of the ICS and NNI system necessary to ensure reliability of the systems and, therefore, minimize the challenges to the plant equipment and operators. The importance of complete system testing, thus ensuring that the system components are adjusted so that the controlled equipment performs its design functions without unnecessary perturbations that challenge the operators and equipment, has been properly emphasized in the general program outlines initiated since the event.

The System Status Reports, Revision 1, were designed to identify the restart testing program. Revision 2 was utilized for final system acceptance and includes system walkdown results, review of maintenance history, trend investigation, and a review of the Davis-Besse SRTP results. The final System Status Reports for both the ICS and NNI system have been reviewed by the staff and found to be acceptable.

Required functional electronics, such as the ICS subsystems, should be calibrated more often than every other refueling, at least until a substantial data base of experience is established, or justification for the scheduled maintenance intervals of every 3 years should be provided. An analysis should be performed by either BWOG or Rancho Seco personnel to demonstrate that the ICS/NNI system power supplies are not susceptible to premature "crowbarring." This analysis could be used as the basis for establishing the surveillance and maintenance schedules for the power supplies. These items need not be resolved by startup, but should be resolved by the next refueling.

Procedures should be revised to ensure that problems discovered during maintenance and testing, such as bad electrical connections and poor soldering on vendor-supplied wiring, are forwarded to BWOG (and INPO and the NRC as appropriate). Conversely, when information from other plants is provided (such as in BAW-1564, the 1979 BWOG recommendations that the reliability of the power supplies associated with the ICS should be improved), that information should be used as a basis to upgrade the surveillance and testing where appropriate.

NNI system functional test STP.1115 and ICS functional test STP.778 have been performed. One wiring error was detected; one faulty module was replaced; and one module that was found to have been inadvertently removed from the ICS was also replaced. STP.664, "ICS/NNI Loss of Power Test," will be performed at hot shutdown. STP.780, "Instrument Cross Correlation Test," has been completed

for cold shutdown and will be performed at hot shutdown and at power. STP.660, "ICS Tuning at Power," will be performed during power escalation. All of these tests will be governed by AP.82, "Conduct of Special Testing," and will be performed as appropriate during restart and power escalation.

Conclusion

The staff finds that the licensee recognizes the importance of proper maintenance, surveillance, and testing for ICS/NNI system and components and actuated equipment, and is taking appropriate measures to implement these activities. These programs of maintenance, surveillance, and testing are acceptable, and this issue is closed as a restart issue.

3.1.2.10 Operator Response and Procedures

Before the December 26, 1985 event, no procedures existed to address the loss of ICS power. The Rancho Seco ATOGs supplied by the B&W Owners Group provide for the loss of ICS and NNI system power but this information was not included in the Rancho Seco EOPs. Following the "lightbulb" incident, loss of NNI system power was addressed in casualty procedures.

As identified in the staff's evaluation of the December 26, 1985 event (NUREG-1195, Section 6, "Personnel Performance"), the operators' responses and procedures were an important element in preventing the event from escalating. Several areas were also identified that demonstrated a need for improvement.

At the time of the event, the on-shift crew was comprised of four Senior Reactor Operators (SROs), one of whom was the Shift Technical Advisor (STA); two Reactor Operators (ROs); and six nonlicensed operators, for a total of twelve operators who were available at the start of the event. Four additional operators who normally would have been available were on vacation. Even considering the people on vacation, the shift crew had five more operators than the minimum number required. This additional staffing, above that required by the Technical Specifications and other licensee commitments, was a significant factor in permitting a number of tasks (isolation of eight valves at four different locations) to be performed simultaneously. With staffing at only the required minimum level, these tasks would have been performed sequentially, would have taken longer to complete, and could have exacerbated the overcooling transient. The licensee has recognized the need for improving operator procedures and training and has initiated corrective actions.

The procedural guidance available to the operators at the time of the event consisted of sympton-based emergency operating procedures (EOPs). The EOPs are based on the plant-specific abnormal transient operating guidelines (ATOGs), which were prepared by the BWOG. The operators used three procedures: E.01, "Immediate Actions"; E.02, "Vital Systems Status Verification"; and E.05, "Excessive Heat Transfer." The existing procedures, at the time of the event, did not address [illegible] of ICS. It was apparent to the NRC staff that the plant operators [illegible] understood the significance of the EOP rules applicable [illegible] 1985 event. The annunciator response procedures for ICS [illegible] used during the event; however, considering the inadequacies [illegible] their use would not have been of any benefit to the operat[illegible] Fan Power Failure" alarm was not appreciated by

the operators because it also acts as a trouble alarm for fan failure and for loss of one of the redundant ICS dc power supplies, neither of which requires immediate operator actions or serves as a transient initiator.

The fact that several licensed operators did not recognize the improper position of the S1 and S2 switches suggests that their training did not adequately focus on normal and off-normal ICS power configurations for this crucial system. According to the operators, neither classroom nor simulator training was provided on the overall plant response to the total loss of ICS dc power or the restoration of ICS dc power, although operators did receive training on mitigating overcooling events with ICS power available. Some problems arose because of the differences between the training simulators and the Rancho Seco control room which were not discussed during operator training. In reviewing the corrective training and procedures, the licensee will assume that the minimum number of operators is available.

In some cases, the operators were unaware of design limitations. For example, most of the non-nuclear instrumentation is independent of the ICS; however, the MFW flow recorders were not. During the event, the recorder indicated a value near mid-scale (because ICS dc power was lost) when MFW flow was actually zero. It is significant that, in spite of concerns raised in recent years, the plant operating staff was unaware of indications that depend on ICS power.

When ICS dc power was lost, the equipment changed its state automatically and operators in the control room lost remote control of ICS-controlled plant equipment. As a result, plant personnel had to go to a variety of locations throughout the plant to operate the ICS-controlled equipment manually (locally); this proved both time consuming and difficult. The operators were also unsure about the status of equipment upon restoration of ICS power. NUREG-1195 also documented the difficulties the operators had with manual valve operation, fences between redundant equipment, and communications.

BWOG Recommendations

Report BAW-1919 makes three general recommendations to prevent complex transients that would significantly ease the need for operator action. These are: ensuring that the plant goes to a known safe state on the loss of ICS, preventing the loss of ICS/NNI system power, and providing unambiguous status and indication.

Appendix J of BAW-1919 ("Recommendation Tracking System, RTS") lists some 207 specific recommendations; of these, several were related to operator response and procedures. This list also gives the priority of each item for each plant. Some of the items include: evaluation of the restoration of ICS/NNI system power, loss of ICS/NNI system power, incorporation of automatic selection of valid input signals, and evaluation of EOPs and plant operating procedures. The staff considers the information included in this listing to be general in nature and useful to particular plants only as a guide.

The BAW-1919 report also includes specific findings from utility reviews in which five general categories of operator burden were noted. The first type of problem involved time-constrained diagnosis, a problem that arises when the operator is asked to make a diagnosis in a relatively short time. Factors that

affect this burden include the complexity of the diagnosis, the availability of the needed input information, the ambiguity of the input, and the lack of clarity in the guidance provided. In a situation of this type, operators generally regress to simple rules. The most recurring comments that reflect this situation are seen in the receipt of hundreds of annunciator alarms upon reactor trip. Many operators stated that they ignore the alarms and concentrate on the response of plant parameters to the transient. The staff notes that, given the confusion of many alarms, it is probably proper for the operator to ignore the alarms until the plant parameters are known and controlled.

The second type of problem, multiple concerns, arises when operators are asked to deal with multiple concerns on an overlapping time scale to the point at which staffing or other constraints makes it difficult to cope with them concurrently. A burden of this type is characterized by the operator fixing his/her attention on resolving a single concern, while neglecting perhaps more important concerns. Operators have identified emergency plan implementation as a burden. The basic concern is that it ties up one or more operators (sometimes the most senior) in such a way that the operator can no longer aid in terminating a transient and stabilizing the plant. The staff considers the prompt notification and implementation of the emergency plan to be necessary, in addition to the other operating duties that must be performed. Another example of this burden involves the loss of the NNI system. Even though the available indications were labeled and detailed in the procedures, operators had a difficult time remembering or finding this indication and using it. Since so many of their "normal" control indications were unavailable, operators spent time looking for available instrumentation. This eventually led to "plant paralysis." The operators were reluctant to change any part of plant status since they did not feel they could adequately control plant response.

The third type of problem, conflict, occurs when the operator is placed in a situation in which the procedure requires an action that appears to oppose his/her fundamental training or institutional basis. A burden of this type is characterized by hesitancy to perform the action and by procedure "stretching," making the procedure fit the operator's bias. In 17 different instances, unnecessary operator burden resulted from procedural conflict. These conflict burdens were caused mostly by lack of attention to detail in the procedures; in three cases, no guidance was included in the procedure for performing a particular action that was required. Although none of these instances contributed significantly to overall burden, they cause confusion and this should be rectified. In the transients, some operators place priority on identifying the event (loss of the NNI system) rather than on identifying the symptom and taking action. Steps in the right direction would be (1) improved training in mitigating integrated transients and (2) full management support for such training.

The fourth type of problem occurs when the operator is continually asked to repeat tasks that give the same results, so that the routine nature of the action and the recurring response causes the operator to anticipate the usual response despite the fact that another response is actually occurring. For example, the operator is asked to take hourly readings on an indicator that rarely changes. Problems involving vigilance can also arise when very rare events actually occur. In this case, the operator spends time reassuring himself that the situation is really occurring, rather than taking prompt action.

The operator must make a continual effort to cross-check available indication during normal and transient operation. The resultant burden placed on the operator is the potential to take incorrect action based on erroneous indication.

The last type of problem, incomprehensible negative feedback, occurs when an operator diagnoses a problem and is sure about its source or cause and then is presented with information that does not confirm the certainty. Such burden is characterized by persistence in reevaluating the nonconfirming data until the problem is solved, possibly to the neglect of other serious problems. For example, a drained pressurizer and a significant subcooling margin is an unexpected plant response, not predicted or found during any previous training or experience.

Rancho Seco Program Modifications

(1) Emergency Operator Procedures

Upon the loss of ICS/NNI system power, the plant will trip in a very short time. The operator will then institute the emergency operating procedures, starting with E.01, "Immediate Actions." After verifying reactor trip, tripping the turbine, and reducing the letdown rate, the operator is directed to procedure E.02. These procedures have been revised to better respond to the event.

Procedure E.02, "Vital System Status Verification," now starts with the caution that if NNI system power is lost, SPDS and EFIC instrumentation shall be used to monitor parameters noted in this procedure. Procedure E.02 checks that all ICS/NNI system power is turned on, but notes that the casualty procedures for restoring power should not be allowed to delay implementation of the rest of the EOPs. If a post-trip condition such as loss of heat transfer is present, procedure E.02 directs the operator to the relevant EOP.

A major change in EOPs occurs in procedure E.05, "Excessive Heat Transfer." Step 1 now includes specific setpoints for pressurizer level or OTSG level or RCS temperature at which the main or auxiliary feedwater pumps which are causing the overcooling must be tripped. The steps to trip the pumps were in place at the time of the event, but the lack of specific direction as to when to trip the pumps contributed directly to the extended overcooling.

(2) Annunciator Response Procedures

The annunciator response procedures for loss of the ICS/NNI system provide a "trouble-shooting" list that includes potential causes, expected changes such as power bus transfers, other annunciator indications, and minor corrective actions such as replacement of fuses. If the steps taken in the annunciator response procedure are not successful in restoring the equipment, the procedure directs the operator to the appropriate casualty procedures. The annunciator procedure also provides the operator with setpoint and actuating device information. For example, the procedure for window 64, "ICS System Failure," directs the operator to casualty procedure C.15 if there are any NNI system failure alarms, and to casualty procedure C.40 if the ICS power monitor indicates the power supplies are lost. The annunciator procedures have been revised by the licensee to reflect the equipment and procedural changes that

have been made to support restart. The annunciator hardware has also been rewired to differentiate between a minor system fault and a system failure.

The loss of power to the ICS/NNI system and the subsequent reactor trip will result in many annunciator alarms. The annunciator procedures reviewed by the staff do not address the potential problem of multiple alarms. Operator training and other indications (IDADS, hierarchy) allow the operator to determine the proper order of response.

The IDADS does not provide any specific ICS/NNI system loss-of-power information, but it does provide a non-specific 120-V ac trouble alarm.

(3) Casualty Procedures

The EOPs will provide the system-oriented procedures intended to stabilize the plant's parameters without necessarily determining the specific initiating root cause. The casualty procedures (CPs) are recovery oriented for returning the plant to an acceptable level of normal operation following completion of applicable EOP steps. For normal operations, the operator would use procedure B.3, "Normal Operations" (Revision 29, June 26, 1987).

The Operations Department will write procedures and the Training Department will conduct training on operator response required upon loss of the signal convertor cabinets A and B. The EFIC will provide control after loss of the cabinets. This change will be completed before restart. The operability findings of the NNI system are described in Revision 2 of the System Status Report.

Current casualty procedure C.15 (Revision 12, December 11, 1987) provides for prompt operator actions to evaluate, determine the cause, and restore conditions to normal following a loss of the NNI-X, NNI-Y, or NNI-Z ac or dc power supply. A single power supply failure should not induce a plant transient, because of the redundant power supplies and the fast ABT. The staff notes that previous events occurred when a single power supply failed during the time the redundant power supply was out of service.

Operating procedure C.15, "Loss of NNI-X, Y, and/or Z Power," is considered by the licensee to be nearly in final form. Revision 11 was a complete rewrite and replaces the old procedures C.15, C.16, and C.17. This procedure provides actions supplementary to the EOPs to control the plant following loss of NNI-X, NNI-Y, and/or NNI-Z power, and provides verification of operability of automatic backup process control systems, actions to provide alternate methods of process control where no automatic backup is provided, identification of alternate instrumentation for use with this and other procedures requiring control room instrumentation, and actions to restore lost NNI system and ICS power after the plant is stabilized.

If the operator starts with procedure C.15 on loss of NNI system power instead of the EOPs, this procedure immediately directs the operator to EOP.01. The casualty procedure cautions the operator to assume that all ICS/NNI system-labeled indicators and recorders are unreliable on loss of NNI system power. After verifying the ICS has tripped, the operator is stepped-through equipment required to obtain and maintain hot shutdown via EFIC and SPDS indications. Revision 12 of CP.15 provides more detailed instructions, such as specific

lights to check and a specific key to use to open the cabinet. Revision 11 simply instructed the operator to verify that the ICS has tripped. The staff considers Revision 12 an improvement over Revision 11. Only after the plant is in a stable condition is recovery of NNI system power to be attempted. The restoration procedure consists of attempting to switch all the power supplies and feeder breakers back on. Power distribution schematics are included in the casualty procedure. After power is restored, the operator is instructed to return control to the ICS. If power cannot be restored and plant management has decided to commence a cooldown, the operator is directed to perform operating procedure B.4.

The licensee considers that OP-C.40, "Loss of ICS Power" (Revision 3, November 23, 1987), is basically complete. Revision 2 (June 22, 1987) represented a complete rewrite of the procedure. The procedure tells operators how to restore ICS power after the plant is stable. The operator is first directed to the EOPs. If the loss of ICS power is accompanied by a loss of NNI system power, the operator is directed to procedure C.15 ("Loss of NNI-X, Y, and/or Z Power"). After the plant is stable, the power switches and feeder breakers are to be checked and once power is restored, the operator can restore equipment to ICS control using this procedure. The power distribution schematics are included in the casualty procedure.

The ICS System Status Report states that the procedures for restoring ICS power were not adequate and have been revised. The licensee has replced the ICS and NNI system static analogue memory modules with memory modules that are programmable upon restoration of power.

Operating procedures are established and operators have received training on establishing and reestablishing RCP seal flow. Since such a variety of potential failure modes exist in ICS/NNI system instruments, the operators are trained to utilize the independent SPDS indications.

Conclusion

The operating procedures have been significantly changed and improved since the December 26, 1985 event, and based on the preceding discussion, such operating procedures are acceptable. The issue of operator response and procedures is closed as a restart issue.

3.1.2.11 ICS/NNI System Interactions With Safety-Related Equipment

Description of Previous System Configuration

Normally, the nuclear industry classifies a system that performs an essential safety function as safety related so that the appropriate requirements and attention can be applied. Generally, credit is taken in the FSAR accident analysis only for systems that are classified as safety related. The ICS and NNI system are not safety related and are considered to have no direct impact on safety equipment. However, when power to the ICS is lost, automatic control of the steam generators is also lost, forcing the operators to take local control at the AFW valves to maintain OTSG level. It is also possible to control the valves from the remote shutdown panel. In addition, the loss of NNI power results in erratic behavior of ICS control.

The NNI system provides inputs to the SPDS. When NNI system power is lost, a reactor trip results and the operator must rely upon the SPDS (and other) indications to monitor the post-trip status. However, some of the SPDS indications are unreliable because they interact with the NNI system.

Role in the December 26, 1985 Event

During the NRC staff investigation of the December 26, 1985 event, the licensee stated that the plant staff does not consider the MSLFL a safety-related system. Recently, in conformance with the NRC equipment qualification rule (10 CFR 50.49), the pressure switches on the individual steamlines for each OTSG (inside the containment building) were removed and "qualified" pressure switches were connected to a sample line on the steam header for each OTSG (outside of the containment building). Special quality assurance procedures are now in force for these switches so as to preserve their "qualified" status. The licensee stated that other components of the MSLFL were also purchased as "qualified." However, the licensee went on to say that for maintenance purposes the MSLFL is listed as a non-safety-related system. There is also an indication that the system was not installed as a safety-related system and that potential problems may exist in the area of separation of electrical cables and circuitry.

In summary, credit is given for successful operation of the MSLFL in the licensing basis for the plant, but apparently it was not classified or treated as a safety-related system. Furthermore, the FSAR analysis assumes the successful operation of the non-safety-related ICS to close the MFW stop valve, and thereby ensure that the safety function is accomplished in a single-failure-proof manner and that the leakage flow is not excessive. There is a normal power supply source and an alternate ac source to the ICS/NNI system cabinets. These two power-supply sources are independent of each other, and there is no tie between the two sources upstream of the automatic bus transfer up to and including the diesel generator buses between the normal and alternate power supply to the ICS/NNI system. A single failure of the ABT will result in loss of power to the ICS and subsequent reactor trip. The licensee has determined that this switch is reliable and should have minimal impact on the number of plant trips. The staff notes, however, that the ABT transfer was interrupted during a previous event involving the loss of NNI power as a result of an improper setpoint. The licensee will ensure that the assumption of reliability is supported by preventive maintenance and surveillance.

The battery chargers H4BGA/B act as the isolation devices between the Class 1 power supply and the Class 2 power on the downstream (ICS/NNI system) side. The staff notes that IEEE accepts these as isolation devices only if they are shown to isolate a faulted load and if periodic testing verifies that the current limiting characteristics have not been compromised or lost. The licensee has confirmed that these devices have been specifically reviewed for use as isolation devices and therefore meet the IEEE criteria. The battery chargers have been retested during this outage to verify that the current limiting capability has been maintained. This current limitation capacity will be tested every 2 years per procedure EM.161. These Class 1E battery chargers have blocking diodes in the output circuit to prevent reverse current flow. The use of these devices is acceptable to the staff.

In the original AFW design, the ICS controlled one of the parallel flow control valves to each steam generator. The other valve is controlled by the SFAS. During the event, the ICS was not available to close the valve; this contributed directly to the overcooling.

BWOG Recommendations

Most of the changes related to the ICS/NNI system recommended by the BWOG in BAW-1919 are directed to increasing the reliability of the ICS/NNI system. The most significant safety equipment interactions after the recommended hardware changes are implemented will be the challenges to safety systems upon failure of the ICS/NNI system. The ICS/NNI system, although not the major contributor to reactor trips (13%), is involved in the complexity of pre/post-trip transient behavior.

The BWOG addressed four different questions when evaluating potential changes (several of these changes overlapped more than one category). The categories are (1) trip reduction, (2) availability improvement, (3) economic benefit, and (4) safety and regulations. The staff considers the reduction of unnecessary reactor trips to benefit all categories.

The ICS inputs that will cause reactor trips are:

- RCS flow
- RCS temperature
- turbine header pressure
- startup feedwater flow
- neutron flux
- feedwater temperature

Of these possible reactor trip functions, the BWOG has recommended removing RCS flow and replacing it with an approximation based on pump status which will allow the removal of the redundant unit load demand to simplify the system. BWOG also recommended removing startup feedwater flow. The NRC staff is evaluating these recommendations and will address the changes in a separate safety evaluation (the BWOG reassessment evaluation).

Some of the other specific hardware changes that are intended to either increase the reliability of the ICS/NNI system or reduce the complexity of transients include deleting the feedwater temperature correction on the FW demand function, removing BTU limits, removing the neutron flux auctioneering from RPS input, removing unused ICS/NNI system hardware, eliminating the automatic plant runback on low main feedwater pump discharge, and removing any control for EFW and ADVs from the ICS/NNI system.

Rancho Seco Modifications

See Sections 3.1.2.1 and 3.1.2.2 for a description of the power distribution for the ICS/NNI system. The affected components are also listed. As detailed in the MPR Associates' sensitivity study, the primary problem that separates the B&W design from other PWR designs is the challenges to safety and operator actions when ICS is disabled. The impact of the ICS on the safety systems is

mostly of the nature of a challenge. Having recognized that, the licensee's action plan has as one of its main objectives reducing the number of challenges to the safety systems. As shown in previous sections, the loss of ICS can result in overcooling and the loss of NNI produces erratic ICS behavior. The most common cause of overfeeding is control system failure. The short-term solution that Rancho Seco is implementing before restart is to trip the ICS immediately upon loss of NNI. The sensitivity study indicates that the B&W design is more sensitive to MFW upsets but not necessarily at a more frequent rate than other designs.

Loss of the ICS/NNI system is now (assuming completion of the EFIC installation, see Section 3.1.3) only able to initiate the condition that triggers the event that independently activates the safety systems. For example, loss of the ICS/NNI system does not require the operator to locally activate AFW. That will be done by EFIC which monitors steam generator condition via independent instrumentation. EFIC controls inventory and pressure using separate pumps, pipes and valves. Similarly the HPI/LPI/SFAS/RPS systems are independent of the ICS/NNI system for initiation or control. In particular, the flow control valve on the AFW is now independent of the ICS.

The NNI system directly interfaces with the following systems:

- reactor coolant system
- makeup and purification system
- secondary plant system (OTSG, MFW, turbine)
- core flood system
- ICS
- annunciators

The RPS and SFAS protection systems provide the ICS/NNI system with significant input for process indication and control. There is also a series of lower order protection systems that also interface with the ICS/NNI system for indication and control. Not necessarily in order of importance, these are:

- RCP power monitors
- turbine/generator protection
- turbine load limit
- MFW pump discharge pressure and trip status
- secondary pressure control (position status of turbine bypass valves)
- MFW pump status
- condenser vacuum and differential pressure status

These systems are interfaced with the ICS/NNI system in such a manner as to prevent ICS/NNI system faults from being reflected back into the protection schemes. Failures within the individual protection schemes may drive the ICS/NNI system and could lead to a plant trip. Operator action would be required to compensate for these failures.

The ICS interfaces with the following systems:

- reactor protection
- NNI
- main steam
- feedwater
- instrument air
- vital electrical bus
- makeup and purification

The NNI system provides 23 process inputs to the ICS. These inputs consist of various combinations of RCS flows and temperatures; OTSG pressures and levels; and feedwater flows, temperatures, and differential pressures. In addition to the NNI inputs, the ICS receives inputs from generator MWe and frequency (currently tuned out of the control scheme) and neutron power (high signal selected in ICS). Each input is buffered to ensure faults are not reflected back to an input source.

A fault within an ICS input source that results in an invalid input signal will drive the ICS process outputs. This can lead to turbine load, feedwater and reactor power mismatches that may trip the reactor. After a reactor trip, the ICS control input requirements are reduced to those needed to control OTSG heat sink, and if necessary the operator can manually control the affected parameter. Of the 23 NNI system process inputs to the ICS, 12 can result in a plant trip as a result of losing one of the two ac or three dc NNI power buses. Since EFIC will be installed, the potential of over- or undercooling due to the loss of power to the ICS/NNI system will be greatly reduced.

Loss of an RPS power supply does not drive the ICS because of the auctioneered input. Loss of the generator MWe can result in driving the ICS control scheme to full generator power. Loss of a specific ICS input such as RPS, MWe, or a single NNI system signal, will be addressed through the BWOG Safety Performance and Improvement Program (SPIP). Modifications are being developed to drive the plant to a known safe condition (hot shutdown) on loss of ac or dc power supplies to either the NNI system or the ICS. These modifications will also eliminate 2 of the 12 NNI-to-ICS inputs that result in a plant trip.

The operator will have adequate information on redundant SPDS channels to verify the plant has stabilized at hot shutdown. See Section 3.1.2.6 for a description of the SPDS indications. Additionally, trended process monitoring independent of NNI and ICS will be provided in the control room to ensure that the plant can be taken to cold shutdown without NNI. Manual operation of some process controls outside the control room will be required; however, the results of these remote manual actions can be monitored from the control room. The items which are affected by NNI are identified on the SPDS display and are not required to be used to deal with a loss of ICS/NNI system power.

Conclusions

With the addition of the EFIC and associated changes, the safety impact on the plant that result from ICS/NNI system problems has been reduced. The primary interface concern remains the ability of the loss of ICS/NNI system to challenge the safety systems. Loss of ICS/NNI system power will continue to result in a plant trip. The ability of the plant and the operators to respond has been substantially improved. The issue of ICS/NNI system interactions with safety-related equipment is closed as a restart issue.

3.1.2.12 Licensee's Re-review of IE Bulletin 79-27 Concerns

On November 10, 1979, an event occurred at the B&W-designed Oconee plant, Unit 3, that involved the loss of a non-Class 1E inverter and failure of its associated automatic bus transfer (ABT) device to transfer loads from the inverter to an alternate regulated 120-V ac power source. The inverter supplied power to the

integrated control system (ICS) and to one channel of the non-nuclear instrumentation (NNI) system. The loss of ICS power caused ICS-controlled equipment to assume its respective failure positions, resulting in underfeeding of the once-through steam generators (OTSGs) by the main feedwater (MFW) system and a reactor trip on reactor coolant system (RCS) high pressure. The loss of NNI system power rendered control room indicators and recorders for the RCS (except for one wide-range RCS pressure recorder) and most secondary plant systems inoperable, causing loss of indication for systems used for decay heat removal and water addition to the reactor vessel and steam generators.

On November 30, 1979, the NRC issued IE Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation." IE Bulletin 79-27 required licensees to review the effects of loss of power to each Class 1E and non-Class 1E bus supplying power to plant instrumentation and controls, and to determine the resulting effect on the capability to achieve a safe (cold) shutdown condition via procedures following the power loss. The review and development of procedures necessary to achieve cold shutdown following bus power failures was also required. The intent of IE Bulletin 79-27 was to ensure that the loss of power to any bus could not result in control system actions that cause a plant upset/transient condition requiring operator action concurrent with the loss of control room information (indications, alarms, etc.) upon which the actions would be based. IE Bulletin 79-27 required that licensees perform and document the following actions for staff review:

(1) Review the Class 1E and non-Class 1E buses supplying power to safety-related and non-safety-related instrumentation and control systems which could affect the ability to achieve a cold shutdown condition using existing procedures or procedures developed under item 2 below. For each bus:

    (a) Identify and review the alarm and/or indication provided in the control room to alert the operator to the loss of power to the bus.

    (b) Identify the instrument and control system loads connected to the bus and evaluate the effects of loss of power to these loads including the ability to achieve a cold shutdown condition.

    (c) Describe any proposed design modifications resulting from these reviews and evaluations, and your proposed schedule for implementing those modifications.

(2) Prepare emergency procedures or review existing ones that will be used by control room operators, including procedures required to achieve a cold shutdown condition, upon loss of power to each Class 1E and non-Class 1E bus supplying power to safety and non-safety related instrument and control systems. The emergency procedures should include:

    (a) the diagnostics/alarm/indicators/symptoms resulting from the review and evaluation conducted to satisfy item 1 above

    (b) the use of alternate indication and/or control circuits which may be powered from other non-Class 1E or Class 1E instrumentation and control buses

(c) methods for restoring power to the bus

Describe any proposed design modifications or administrative controls to be implemented resulting from these procedures, and provide your proposed schedule for implementing the changes.

(3) Re-review IE Circular No. 79-02, "Failure of 120 Volt Vital AC Power Supplies," dated January 11, 1979, to include both Class 1E and non-Class 1E safety-related power supply inverters. On the basis of a review of operating experience and your re-review of IE Circular No. 79-02, describe any proposed design modifications or administrative controls to be implemented as a result of the re-review.

The licensee's response to IE Bulletin 79-27 (Sacramento Municipal Utility District (SMUD) letter dated February 22, 1980) concerning item 1c stated that no design modifications were necessary based on the results of their review. The results of the review concerning loss of power to ICS and NNI loads were:

(ICS) The effect of a loss of power to the ICS will result in a power transfer of the ICS via an automatic transfer to a non-Class 1E bus. Therefore, a loss of power on this channel will have no effect on the operation of the ICS. However, if the assumption is taken that a non-1E bus is not available, then the ICS failure response is that all controlled devices will revert to their 50% position.

(NNI) Each source of power, one to the "X" supply and one to the "Y," is backed with an automatic transfer switch. If the entire source was lost, both would be transferred to a non-Class 1E bus. Therefore, no adverse effects would be noted.

The licensee's response concerning item 2 of IE Bulletin 79-27 was:

> As described in response to Question 1.b upon loss of power to each Class 1E and non-Class 1E bus supplying power to safety- and non-safety-related instrument and control systems that may be required to achieve a cold shutdown condition there is an automatic transfer to another power source. Therefore, no additional emergency procedures are required.

On February 26, 1980, an event occurred at the B&W-designed Crystal River, Unit 3 nuclear plant, that involved a loss of NNI system power. Failed input signals provided to the ICS from the NNI system caused RCS overpressurization and the subsequent release (blowdown) of more than 40,000 gallons of reactor coolant into the reactor building through the pressurizer power-operated relief valve (PORV) and the reactor coolant drain tank rupture disc. The loss of power also resulted in the failure of most of the instruments needed by the operator to respond to the event, making operator action very difficult.

The event at Crystal River involved the types of concerns that the staff was trying to eliminate through the licensee reviews required by IE Bulletin 79-27. By letter dated March 6, 1980, the staff required all licensees of B&W-designed reactors to expand the review of IE Bulletin 79-27 to include the implications of the Crystal River event. On March 7, 1980, the staff issued IE Information

Notice 80-07, which described the Crystal River event and stated that IE Bulletin 79-27 was intended to cause licensees to investigate the loss of individual power supplies as well as the loss of inverters and vital buses. The results of the licensee's expanded review of IE Bulletin 79-27 (SMUD letter dated March 12, 1980) did not change the conclusions reached during their initial IE Bulletin 79-27 review.

On March 19, 1984, an event occurred at the B&W-designed Rancho Seco nuclear plant that involved a partial loss of NNI system power (specifically NNI-X ±24-V dc power). The loss of power was the result of a single failure of an inverter, and undetected drift of an NNI system 24-V dc power supply internal overvoltage protection ("crowbar") circuit setpoint. At the time of the event, the control room indicators which provided essentially all primary and secondary system status information to the operators received inputs from and were powered by the non-nuclear instrumentation. The loss of power resulted in mid-scale failures of numerous indicators. The operators manually initiated high-pressure injection by using the wrong procedure, and pressurized the reactor coolant system to the point where a pressurizer code safety valve opened twice. The loss of NNI system power occurred approximately 1 hour after a reactor trip had occurred. The ICS responded to the power loss by signaling an atmospheric dump valve (ADV) to open. Since ICS power remained available during this event, the operators were able to place the ADV controls in the manual mode (taking automatic control of the ADV away from the ICS) to close the valve. This event also involved the types of concerns addressed by IE Bulletin 79-27, and subsequently addressed in the staff's March 6, 1980 letter, and IE Information Notice 80-07.

On December 26, 1985, an event occurred at Rancho Seco that involved a loss of ICS ±24-V dc power. Upon loss of ICS dc power, equipment control modules lost power and provided zero (0-V) dc outputs, and switching relays lost power (going to the de-energized state). This not only caused ICS-controlled plant equipment to change positions, initiating a plant transient, but also caused the loss of remote manual control of key ICS-controlled plant equipment from the control room. Furthermore, the operators were misled by an MFW flow recorder that had failed to the mid-scale position upon the loss of power.

The incident at Rancho Seco on December 26, 1985 was significant because it again demonstrated that a single failure in the non-safety-related ICS/NNI system system could subject the plant to an undesirable transient and challenge the operator's capability to mitigate the transient without resulting in primary system undercooling or overcooling. The event also demonstrated that the concerns addressed through IE Bulletin 79-27 continued to exist at B&W-designed reactors. The event at Rancho Seco involved a loss of power that caused control system actions resulting in a significant plant transient, and a failure of control room indications used by the operators to respond to the transient. The staff believes that a careful and thorough review of plant designs in accordance with IE Bulletin 79-27 would detect the potential for this type of event, and result in hardware and/or procedural modifications to ensure that a safe shutdown condition could be achieved following the power loss. A review of the licensee's original response to IE Bulletin 79-27 in light of the December 26, 1985 event revealed several deficiencies, including:

(1) The non-existence of specific procedures concerning the loss of ICS power. Such procedures could provide direction for restoration of power to regain manual control of ICS-controlled equipment, identify appropriate indications to be used and/or avoided by the operators, and direct the operators to alternate points of control for achieving and maintaining cold shutdown. The B&W symptom-oriented abnormal transient operating guidelines (ATOGs) include a section entitled, "Loss of NNI/ICS," which deals with control of the plant without NNI system or ICS power, but the ICS portion of that procedure had not been incorporated into the licensee's emergency or casualty procedures as a separate entity. It is noted that some of the steps from the ATOG procedures concerning loss of ICS power were included in Rancho Seco emergency operating procedure E 05, "Excessive Heat Transfer"; but this procedure is not sufficient for proceeding to cold shutdown and does not satisfy item 2 of IE Bulletin 79-27.

(2) Taking credit for automatic bus transfer (ABT) or switching devices to transfer power to bus loads from the normal source to an alternate/standby source upon failure of the normal source. This assumption is inconsistent with the requirement of item 1b of IE Bulletin 79-27, and is not acceptable for analyzing the effects of loss of power to loads due to bus faults, which can occur regardless of the number of sources feeding the bus through ABT devices or auctioneering techniques.

Additional information regarding the licensee's review of IE Bulletin 79-27, and the staff's evaluation of the licensee's review is provided in Section 7, "Precursors to the December 26, 1985 Incident at Rancho Seco and Related NRC and SMUD Actions," of NUREG-1195, "Loss of Integrated Control System Power and Overcooling Transient at Rancho Seco on December 26, 1985."

Because of the deficiencies identified in the original IE Bulletin 79-27 review, the staff required the licensee to re-review the Rancho Seco plant design in accordance with IE Bulletin 79-27. The re-review was to be performed before restart following the December 26, 1985 event. The re-review was intended to ensure identification of all bus power losses/power supply failures that could potentially prevent the control room operators from achieving a safe (cold) shutdown condition through the use of existing plant procedures, and to implement any necessary hardware and/or procedural changes. The re-review was also needed to account for a number of plant changes made in preparation for restart that affected the plant electrical distribution system. The changes included installation of new emergency diesel generators, inverters, battery chargers, etc., and the reassignment of some electrical loads.

Evaluation

Information concerning the re-review of IE Bulletin 79-27 for the Rancho Seco plant was provided to the NRC by SMUD letters dated October 12 and December 24, 1987. The staff's evaluation of the adequacy of the licensee's re-review is primarily based on the review of information provided in these letters and information obtained during a site audit of the re-review methodology on December 15, 1987.

The licensee re-reviewed the Rancho Seco plant design to determine the impact of single instrumentation and control system power bus failures on the ability

to achieve a cold shutdown condition through the use of plant procedures. The licensee has stated that all Class 1E and non-Class 1E ac and dc buses providing power to plant instruments and controls were included in the IE Bulletin 79-27 re-review. The licensee evaluated 47 individual bus failures. For most failures, the plant can proceed to cold shutdown with minimal problems by using backup equipment. However, the re-review did identify several bus power losses for which the capability to achieve cold shutdown using existing plant procedures was significantly impaired, and for which hardware and/or procedural changes were considered necessary. The licensee stated that the IE Bulletin 79-27 re-review used the latest plant design information, and thus accurately reflects the plant configuration that will exist as of plant restart.

The methodology used by the licensee during the IE Bulletin 79-27 re-review was to evaluate the effects of the loss of power to each bus individually by analyzing the combined effects of loss of power to all bus loads (instruments, controls, pumps, valves, etc.) and the resulting effect on the ability to proceed to cold shutdown using normal procedures. The re-review included an evaluation of the indication/annunciation provided to alert the operator in the control room to the bus power loss. All equipment/component losses due to the failure of each individual bus were evaluated along with all equipment/component losses due to the consequential failure of all connected buses. Thus, the cumulative effects of loss of power to all loads affected by a loss of bus power, including the loss of power to loads due to cascading power losses, were considered simultaneously to determine the overall effect on the plant during power operation. The analysis was not restricted to loads used to achieve plant shutdown via procedures.

For each bus designed to receive power from multiple sources via automatic bus transfer (ABT) devices, static switches or similar devices, the IE Bulletin 79-27 re-review analyzed the effect of loss of power to the bus as described above (i.e., bus faults were considered; credit was not assumed for automatic transfer device operation to prevent loss of power). The consideration of loss of power to buses supplied from multiple sources via automatic transfers is a major improvement over the original IE Bulletin 79-27 review in which these buses were assumed not to fail because of input source redundancy. The licensee only assumed credit for ABT or static switch operation for situations where an upstream bus failure results in loss of the normal supply to a downstream bus, and the transfer device operates to maintain bus power from the alternate/standby supply. In this case, the failure of the automatic transfer device would constitute a second failure. The staff concludes that taking credit for the automatic transfer device in this situation is acceptable provided that periodic maintenance and surveillance are performed to verify its operability, and thus provide reasonable assurance that the device will function properly when needed. The licensee has indicated that the Rancho Seco plant administrative/operating procedures ensure the availability of bus transfer devices. Preventive maintenance is performed during each refueling outage for inverters and transfer switches, and once per year for the ICS/NNI systemsystem ABT devices. The Rancho Seco plant casualty procedures for power bus failures require the operator to check that lower level buses supplied via automatic transfer devices remain operable, and if not, directions are provided for the correct operator response. The failure of each battery-backed bus was also considered during the IE Bulletin 79-27 re-review. Battery-backed buses were assumed to remain available

following upstream power losses only if an independent alternate feed to the bus was available.

Casualty procedures have been written or reviewed and revised as required to provide the operator with the correct response and recovery actions to mitigate the consequences of loss of power to each bus. If a loss of bus power occurs during normal reactor power operation, the corresponding casualty procedure directs the operator to take action to stabilize the plant using the equipment and instruments that remain available. If the operator cannot stabilize the plant following the bus power loss and plant parameters reach a point requiring a reactor trip, the reactor may be tripped manually, or the safety-related reactor protection system (RPS) will automatically initiate a reactor trip before plant conditions exceed safe operating limits. Therefore, the procedures reviewed as part of the IE Bulletin 79-27 re-review were the individual bus casualty procedures, emergency operating procedure (EOP) E.01, "Immediate Actions," used to maintain the reactor in a safe condition following a reactor trip; EOP E.02, "Vital System Status Verification," used to ensure that the plant achieves a stable condition within the B&W ATOG post-trip pressure-temperature window; and plant control procedure B.4, "Plant Shutdown and Cooldown," used to achieve final plant cooldown to cold shutdown conditions.

Therefore, for each bus power loss, the licensee reviewed the procedures used by the operators to respond to the power loss and to obtain subsequent cold shutdown of the plant. In order to evaluate the impact of bus failures on the ability to achieve cold shutdown, a list was prepared that identified all equipment specifically referenced by procedures E.01, E.02, and B.4. Other plant auxiliary/support systems were reviewed to further determine the availability of equipment referenced by these procedures following power losses. The equipment list was then used for each single bus failure evaluation to identify those procedure steps for which equipment unavailability due to the power loss requires that the operator take alternate action. The procedures were then revised to provide guidance to the operators concerning redundant equipment or instrumentation for use in continuing the plant cooldown with the normal procedures. The licensee considered the use of EOPs other than E.01 and E.02 to be unacceptable for achieving stable plant conditions following individual bus failures. The results of the IE Bulletin 79-27 re-review indicate that hot shutdown can be achieved following a plant trip through procedures E.01 and E.02 without using plant procedures other than the respective bus casualty procedure(s).

Procedure B.4 provides two methods for achieving cold shutdown: forced circulation cooling and natural circulation cooling. The IE Bulletin 79-27 re-review assumed that either cooldown method was acceptable in achieving cold shutdown following bus failures.

In addition, the re-review considered restoration of power to bus loads to be an acceptable option during plant cooldown via procedure B.4 (since no time limit is imposed) if it can be demonstrated that the plant can be maintained in a stable condition. The staff prefers the use of alternate redundant equipment that is unaffected by the bus power loss to reliance on restoration of power to continue plant cooldown. The desirability of restoration of power is recognized, and it is assumed that the operator would first attempt to restore power as directed by the casualty procedures. However, it cannot be assumed that

power can be restored within a reasonable time. In several cases during the IE Bulletin 79-27 re-review, the licensee takes credit for equipment to be disconnected from its normal bus, and power provided to the equipment from a redundant bus via temporary connections in accordance with revised procedures. The staff believes that for these situations, hardware design modifications (e.g., the reassignment of loads or the provision of redundant equipment unaffected by the power loss) are clearly more desirable. However, the staff has accepted the above approach for several limited cases (discussed later in this section) for the interim pending plant modifications.

The licensee's re-review of IE Bulletin 79-27 was divided into two parts: (1) ICS/NNI system bus power losses and (2) all other bus power losses.

The licensee's approach to ensuring that ICS/NNI system power losses will no longer result in plant transient conditions requiring operator actions concurrent with the loss of instrumentation and controls needed to accomplish the actions, is discussed in detail in Section 3.1.2.6, "Loss of Control Room Controls and Indications and Adequacy of Backup Instrumentation," of this report. This approach is summarized below.

The licensee has modified the ICS/NNI power system design so that any loss of NNI system ac or dc power or the loss of ICS ac power will result in a forced automatic trip of the ICS dc power supplies. This will allow the control room operator to concentrate on a common response for all ICS/NNI system power failures. The licensee has also installed circuitry to automatically trip the MFW pump turbines on loss of ICS ac or dc power. The trip of both MFW pumps will in turn cause a reactor trip. Circuitry to initiate a reactor trip on an MFW pump trip was installed in accordance with TMI Action Plan Item II.K.2.10, "Safety Grade Anticipatory Reactor Trip," of NUREG-0737, "Clarification of TMI Action Plan Requirements." The operators are trained to initiate auxiliary feedwater (AFW) flow to the OTSGs upon receipt of ICS/NNI system power failure alarms and MFW pump trip alarms. Clear indication of the loss of ICS/NNI system power is provided by control room alarms as discussed in Sections 3.1.2.2 and 3.1.2.3 of this report. In the absence of operator action, the newly installed safety-related emergency feedwater initiation and control (EFIC) system will automatically initiate AFW flow to the OTSGs upon detecting a low water level, and will control OTSG level and pressure. These modifications are designed to provide the capability to establish controlled heat removal from the reactor coolant system (RCS) following a loss of ICS and/or NNI system ac or dc power by automatically placing the plant in the B&W ATOG "post-trip" window (i.e., a known safe state as defined by the EOPs). The primary function of the control room operator will be to verify that the automatic actions (trip of the MFW pumps and automatic initiation of AFW by the EFIC system) have occurred, and that stable plant conditions are achieved within the "post-trip" window.

The staff reviewed the backup instrumentation and controls used by the control room operators to control and shut down the plant following a loss of ICS/NNI system power. For each instance in which an ICS/NNI system indication or control is used by the operators to bring the plant to a hot-shutdown or cold-shutdown condition, a backup indication or control independent of the ICS and NNI system is provided. In addition, the licensee has developed and/or revised the casualty procedures for loss of ICS/NNI system power as discussed in Section 3.1.2.8 of this report.

The staff concludes that the ICS/NNI system design modifications described above, and the associated procedural changes are sufficient to (1) prevent a loss of ICS/NNI power from causing a plant transient requiring operator actions concurrent with the loss of control room indications and controls needed to accomplish the actions and (2) allow the operators to achieve subsequent cold-shutdown conditions through the use of plant procedures.

The licensee reviewed all other bus failures (i.e., non-ICS/NNI buses) at the 4160-V ac level and below in accordance with the methodology described above. The following bus designation prefixes are used at Rancho Seco:

S4 - 4160-V ac
S3 - 480-V ac (load center)
S2 - 480-V ac (motor control center)
S1 - 120-V ac
SD - 125-V dc

As part of the IE Bulletin 79-27 re-review, the licensee identified the alarms and/or indication provided in the control room to alert the operator to loss of power for each bus. Clear, concise, non-confusing indication of bus failures is important to quickly direct the operators to the proper casualty procedure. In general, the casualty procedures are referenced by the annunciator response procedures. Clear, unambiguous indication of loss of bus power is provided in the main control room for most bus failures. In general, the indication is provided by main annunciator system alarm points or by interim data acquisition and display system (IDADS) alarms. The IDADS is a plant process computer system that monitors plant conditions and performs various calculation, trending, alarm, indication, and post-transient data logging functions.

However, for certain buses, the control room indication of loss of bus power may not be sufficient to allow easy identification of the specific bus failure. For six instrument buses (S1A2-1, S1B2-1, S1GA-1, S1GB-1, S1N1-1, and SOE), a loss of bus power will also result in loss of the bus failure annunciation because the alarm circuits receive power from the buses themselves. The licensee believes that the loss-of-power alarms for these buses need not be modified for plant restart because loss of the bus either does not require immediate notification of the operator, or has unique symptoms which lead the operator to timely diagnosis of the problem. The licensee has stated that for four of the buses (S1A2-1, S1B2-1, S1GB-1, and S1N1-1), the plant can be brought to hot shutdown by using EOPs E.01 and E.02 without the bus. Once the plant is in hot shutdown, other indications and alarms can be used to diagnose the bus failure and allow the operator to take subsequent actions in accordance with the correct procedures. The loss of power to bus S1GA-1 results in the loss of control power to both auxiliary boilers. The licensee has stated that an operator is always dispatched to the auxiliary boilers following a reactor trip and that the operator would quickly realize that power was lost which would lead to quick diagnosis of the failed bus. The licensee has stated that loss of the auxiliary boilers has no effect on the ability to achieve hot shutdown or plant cooldown to cold shutdown. The loss of bus SOE will cause a reactor trip and the loss of all main annunciators. This is a unique combination of events that can only occur if bus SOE fails. The operators are trained for this event, and the licensee believes that the specific bus failure will be quickly recognized.

The licensee is considering installation of alarms to provide clear unambiguous indication of power failure for the six buses discussed above. The licensee considers installation of the alarms to be a priority 2 modification (i.e., installation following plant restart is acceptable). Priority 1 modifications require implementation before plant restart, because in the absence of the modification one of following could occur:

- technical specification violation
- plant operation outside of the ATOG post-trip window
- operator action required outside of the control room within the first 10 minutes following a reactor trip

The staff considers installation of the alarms to be necessary to minimize the operator burden involved in detecting the specific bus power loss and in taking the appropriate actions necessary to achieve plant shutdown through the proper procedures (E.01, E.02, and B.4). The staff finds the priority 2 categorization for installation of the alarms to be acceptable based on the other means that exist for the operators to identify the specific bus failure, and that the plant response to the failure will not result in plant operation outside of established safe operating limits or the ATOG post-trip window, and will not prevent subsequent cold shutdown through the use of normal procedures.

Therefore, the staff concludes that plant operation in the interim is acceptable pending modifications to provide the alarms.

The staff reviewed two cases during its audit review where a single annunciator point was used to indicate the failure of more than one bus. For the cases reviewed, the annunciator response procedures contained clear guidance for the operators to determine the specific bus failure that caused the alarm.

The staff audited the licensee's IE Bulletin 79-27 re-review at the Rancho Seco site on December 15, 1987. The audit included the review of plant electrical distribution system one-line diagrams, EOPs, annunciator response procedures, and casualty procedures. Two specific bus failures reviewed during the audit were 4160-V ac bus S4A2 and 125-V dc bus S0E. These buses were chosen for the audit review because their failure appeared to represent potentially worst-case scenarios as far as the number and complexity of operator actions required to stabilize the plant and/or achieve safe (cold) plant shutodwn following a reactor trip.

The failure of bus S4A2 also involves the loss of power to many lower level buses through cascading power losses. Buses S3A2, S2A2, S2A4, S2A3, S1A3, and S1A4; battery chargers H4BA2, H4BC2, and H4BAC; and inverter S1GA to buses S1GA-1 and S1J are all assumed to lose power along with bus S4A2. The staff performed a cursory review that identified the loads connected to these buses, and reviewed the effects of loss of power to the loads on the capability to achieve plant shutdown through EOPs E.01 and E.02, and plant control procedure B.4. Bus S4A2 is backed by emergency diesel generator (EDG) GEA2; no credit was taken for automatic start of the EDG to supply bus loads. The indication provided in the control room to alert the operators to the power losses appeared to be adequate. The IDADS provides separate loss of power alarms for most of the failed buses. Several plant casualty procedures were reviewed for specific buses or failed equipment. The casualty procedures were found to

contain appropriate guidance for restoration of power, identification of inoperable equipment and indications, and associated corrective actions. It was noted that the annunciator response procedure for "NON-VITAL POWER BUS 1E/1F/1J TROUBLE" needed revision to refer to the appropriate casualty procedure(s). The licensee indicated that the annunciator response procedures are currently being revised, and that the appropriate corrections would be made before plant restart. It appears that the licensee has carefully evaluated the combined effect of loss of power to all loads on plant operation and ability to achieve shutdown, and has made appropriate procedural changes where necessary. The results of the licensee's analysis appear correct.

Failure of bus SOE appears to represent the most difficult loss of bus power event in terms of achieving plant shutdown through procedures. Loss of power to SOE results in a number of undesirable effects, including loss of control room annunciators, loss of capability to transfer loads from the unit auxiliary transformer to the startup transformer, loss of electromagnetic relief valve (EMOV) control, loss of the Bailey computer, loss of the ac and dc reactor coolant pump lift oil pumps, miscellaneous equipment failures, and mid-scale failures of some control room indicators. Loss of bus SOE will cause both MFW pumps to go to zero speed, and will result in a reactor trip and turbine trip. There is no dedicated control room indication of the failure of bus SOE. The licensee indicated that the operators receive extensive training for this event; the combination of a reactor trip and loss of the main annunciators keys the operators to the failure. Casualty procedure C.154 "Loss of 125-V dc Non-vital Bus SOE," directs the operator's response to this event following completion of EOPs E.01 and E.02. The failure of bus SOE is similar in many respects to a loss of offsite power, and loss of the unit startup transformer. Casualty procedure C.154 has been revised and appears to be sufficient to allow the operators to safely shut down the plant, although the procedure seems to be fairly difficult to follow and certain hardware modifications are desirable, as discussed below. The licensee indicated that proposed modifications are being considered (including installation of an ABT device to provide power to the annunciators from a standby source upon loss of power) and will likely be implemented after plant restart.

Loss of power to bus SOE results in loss of remote manual and automatic control for the EMOV. The EMOV is required to be available by procedure B.4 during plant cooldown to provide low-temperature overpressure protection (LTOP). The staff reviewed the use of a special pre-cut cable to be permanently stored in vital area 10 and to be used to provide power to the EMOV from 125-V dc bus SOF upon loss of bus SOE. Buses SOE and SOF are located in separate rooms of vital area 10. Two security/fire doors must be left open when this cable is in use. Connection of the cable takes approximately 20 minutes and must be performed by an electrical technician upon request from the operators using the casualty procedures. Connection involves disconnecting the EMOV from bus SOE and reconnecting it to one end of the cable, and connecting the other end of the cable to bus SOF (all connections are made using pressure/compression-type screw lugs). Sufficient time exists for connecting the cable before reaching the point in procedure B.4 where LTOP is required. While this fix (use of a temporary cable via procedures) can be used to attain cold shutdown, a hardware modification to prevent the need for such an operation is considered preferable, as discussed below.

There are several bus failures that can result in the loss of remote manual control capability for core flood tank isolation valves or decay heat removal (DHR) system dropline isolation valves. The licensee intends to provide power to these valves when required during plant cooldown by use of a special power cart. The cart is normally used to perform 80% voltage valve operability tests. The cart itself receives power from room 480-V ac receptacles powered from a motor control center (MCC) independent of the MCC normally providing valve power. Power is, in turn, provided from the cart to the valve motor from its 480-V ac switchgear breaker cubicle, after the normal supply has been disconnected. As with the cable above, the cart must be used by electrical technicians upon operator request via the casualty procedures. Connection of the cart takes approximately 30 to 40 minutes. The licensee indicates that sufficient time exists to make the necessary connections. The cart will be dedicated to the respective switchgear rooms. The cart's location is controlled by administrative procedures. Although the use of temporary connections via the power cart and revised procedures appears adequate for providing power to the subject valves to regain operability for cold shutdown, plant hardware should be modified on a priority basis to prevent the need for such connections.

The use of temporary connections such as the cable and power cart discussed above, present additional risk to plant personnel and plant equipment, and place increased burden on the control room operator in achieving cold shutdown. The staff does not consider such temporary connections to be acceptable engineering or operational practice for use on a permanent basis. Permanent hardware modifications should be made to eliminate reliance on these techniques. The licensee has indicated its intent to implement such hardware modifications after plant restart. The modifications are considered priority 2, and should be implemented before startup following the first refueling outage after plant restart.

It should be noted that seven different bus failures can result in the loss of the auxiliary boilers. If the plant is at a very low decay heat generation rate, the potential for excessive heat transfer from the primary to the secondary plant exists, since the steam drain will exceed the decay heat generation rate. The licensee contends that the loss of the auxiliary boilers do not affect the ability to achieve safe shutdown or cooldown:

> The main steam system can be used, except at very low RCS temperatures, to provide steam for necessary loads such as gland steam and air ejectors, thus, the loss of auxiliary boilers has no affect on the ability to achieve hot shutdown or cooldown to cold shutdown. The casualty procedures, including applicable loss of bus procedure and loss of auxiliary boiler procedure, provide direction to the operator to isolate steam loads to prevent excessive cooldown as a result of auxiliary boiler unavailability.

The procedural solution appears to be sufficient to terminate the excessive heat transfer condition, but hardware modifications to prevent a single bus failure from resulting in a loss of both auxiliary boilers should be considered.

The licensee's re-review of IE Bulletin 79-27 has considered the loss of power to each bus, as well as the failure of all connected loads, including connected power sources. All Class 1E and non-Class 1E inverters were considered

in the re-review. The licensee has indicated that all inverters, static switches, automatic bus transfer devices, etc., receive routine electrical maintenance to ensure their operability. The staff reviewed the electrical maintenance (EM) procedure for inverters S1A2 and S1B2, which states: "If inverter has an automatic transfer scheme, check and time transfer from inverter to alternative source." However, as noted during the staff audit, the associated signoff data sheet does not include spaces to record the "as found" and "as left" automatic transfer point and transfer time. The licensee implied that the EM for S1A2 and S1B2 is typical for all inverters and automatic bus transfer devices and that changes would be considered. The staff concludes that the licensee's re-review of IE Circular 79-02, "Failure of 120 Volt Vital AC Power Supplies," as required by IE Bulletin 79-27 is acceptable, but that the EM procedures should be revised as discussed above.

Conclusions

On the basis of its review of the licensee's re-review of IE Bulletin 79-27, the staff concludes that there is reasonable assurance that the failure of any single Class 1E or non-Class 1E bus that supplies power to plant instrumentation and controls will not result in a plant transient condition requiring operator action and the simultaneous loss of control room indications on which the actions would be based. The staff further concludes that there is reasonable assurance that a safe (cold) plant shutdown condition can be achieved following loss of power to any Class 1E or non-Class 1E bus providing power to plant instruments and controls, by using EOPs E.01 and E.02, shutdown procedure B.4, and the plant casualty procedure(s) applicable to the specific bus failure. It appears that the licensee has performed a careful and thorough review of both the ICS/NNI system power buses and all other plant power buses. Numerous procedural changes have resulted from the review, and in the case of the ICS/NNI system, substantial hardware modifications have also been made. The staff concludes that these hardware and procedural changes will result in a significant improvement in plant safety with regard to the ability to achieve a cold shutdown following the loss of power to any bus. The staff concludes that the IE Bulletin 79-27 re-review methodology used by the licensee was sound with regard to the review of plant procedures and the treatment of cascading power losses and the operation of ABT and similar devices. On this basis, the staff considers the Rancho Seco design acceptable for plant restart following the December 26, 1985 loss of ICS power and overcooling event with respect to the concerns addressed by IE Bulletin 79-27. The issue of IE Bulletin 79-27 re-review is closed as a restart issue.

3.1.3 Emergency Feedwater Initiation and Control System

The postaccident design review by the Nuclear Regulatory Commission (NRC) after the March 28, 1979 accident at the Three Mile Island (TMI) Nuclear Station, Unit 2, established that the auxiliary feedwater (AFW) system should be designed, implemented and maintained as a safety system.

To improve the reliability of AFW systems, the NRC required all utilities to upgrade existing AFW systems, where necessary, to ensure timely automatic initiation when required. The upgrade involved qualifying the automatic initiation signals and circuits in accordance with safety-grade requirements. Item II.E.1.2, "Auxiliary Feedwater System Automatic Initiation and Flow Indication,"

of NUREG-0737, "Clarification of TMI Action Plan Requirements," specifies that this objective can be met by the installation of an AFW actuation system that conforms to the requirements of IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," and provides the following set of minimum requirements.

(1) The design shall provide for the automatic initiation of the AFW system,

(2) Automatic initiation signals and circuits shall be designed so that a single failure will not result in the loss of AFW system function,

(3) Testability of the initiating signals and circuits shall be a feature of the design,

(4) Initiating signals and circuits shall be powered from the emergency buses,

(5) Manual capability to initiate the AFW system from the control room shall be retained and shall 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 AFW system shall be included in the automatic actuation (simultaneous and/or sequential) of the loads to the emergency buses, and

(7) Automatic initiating 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.

Item II.E.1.2 of NUREG-0737 also required that safety-grade indication of auxiliary feedwater flow to each steam generator be provided in the control room. For Babcock and Wilcox (B&W)-designed plants such as Rancho Seco, a minimum of two AFW flow-rate indicators for each steam generator must be provided. The auxiliary feedwater flow instrument channels are to be powered from the emergency buses.

In addition, Item II.K.2.2, "Control of Auxiliary Feedwater Independent of the Integrated Control System," of NUREG-0737 requires that licensees of B&W-designed reactors provide procedures and training to initiate and control AFW independent of the non-safety related integrated control system (ICS).

The information in this section supersedes that contained in Section 3.1.3 of the Rancho Seco Restart SER (October 1987).

Description of Auxiliary Feedwater System

The AFW system provides secondary coolant to the once through steam generators (OTSGs) if the main feedwater (MFW) system becomes unable to perform this function or if AFW is needed to promote natural circulation in the reactor coolant system. When monitored plant parameters indicate the need for it, the emergency feedwater initiation and control (EFIC) system will automatically initiate AFW flow to the OTSGs. The AFW system may also be initiated manually at the discretion of the operator. Following AFW system actuation, the EFIC

system is designed to automatically control the levels in the OTSGs at one of three possible setpoints, depending upon the actual plant conditions.

The AFW system consists of two interconnected flowpaths/trains. Each train is capable of supplying auxiliary feedwater to either or both OTSGs. Figure 3.5 (revised) is a flow diagram of the Rancho Seco AFW system. This figure also identifies the EFIC system control signals to AFW system components.

The AFW system is designed to provide a minimum of 475 gpm of AFW to the OTSGs at 1050 psig within 70 seconds of a system initiation signal. Before restart, flow-restricting venturis will be installed in the AFW system injection lines.

Flow for AFW system train A (which supplies AFW to OTSG B and OTSG A) is normally provided by pump P-319; train B flow (supplied to OTSG A and OSTB B) is normally provided by pump P-318. Each pump has a rated capacity of 840 gpm at 1150 psig and a normal minimum flow recirculation of 60 gpm. Either of the pumps can provide the required system flow rate to both OTSGs. AFW system pump P-318 is a combination turbine/motor-driven pump has the turbine and motor mounted on a common shaft. Either motive force can drive the pump at rated capacity. The primary motive force which receives an automatic start signal is the turbine. The motor drive is not automatically initiated, but can be started by the control room operator. AFW system pump P-319 is strictly a motor-driven pump.

The steam supply for pump P-318 turbine (K-308) is obtained from both OTSGs through 6-inch lines that contain check valves, locked open manual valves, and motor-operated valves. The check valve and motor-operated valve associated with each OTSG provide redundant isolation capability to preclude blowing down the good OTSG in the event that a rupture (main steamline or main feedwater line) occurs in an OTSG.

Normally, ac power for the pump P-319 motor is provided by 4160-V bus 4A2 through switchgear S4A2, with emergency backup power provided by emergency diesel generator A (GEA2). The ac power for the pump P-318 motor is normally provided by 4160-V bus 4B2 through switchgear S4B2, and emergency backup power is provided by emergency diesel generator B (GEB2).

The primary water source for both AFW trains is the seismic Category I condensate storage tank (CST), which has a minimum capacity of 250,000 gallons. Backup sources of water are available from the onsite reservoir and the Folsom South Canal.

Isolation valves, control valves, check valves, and flow instruments are located in the flowpaths between the AFW pumps and the OTSGs to monitor and control the flow of AFW to the OTSGs.

The EFIC system determines the need for AFW; initiates AFW by starting the pumps and opening valves, as necessary, to provide a flowpath to the OTSGs; and controls the flow of AFW to maintain the proper water level in the OTSGs.

3.1.3.1 EFIC System Design and Operation

The EFIC system at Rancho Seco is a four-channel, safety-grade, seismically qualified and Class 1E AFW initiation and control system. The EFIC system also

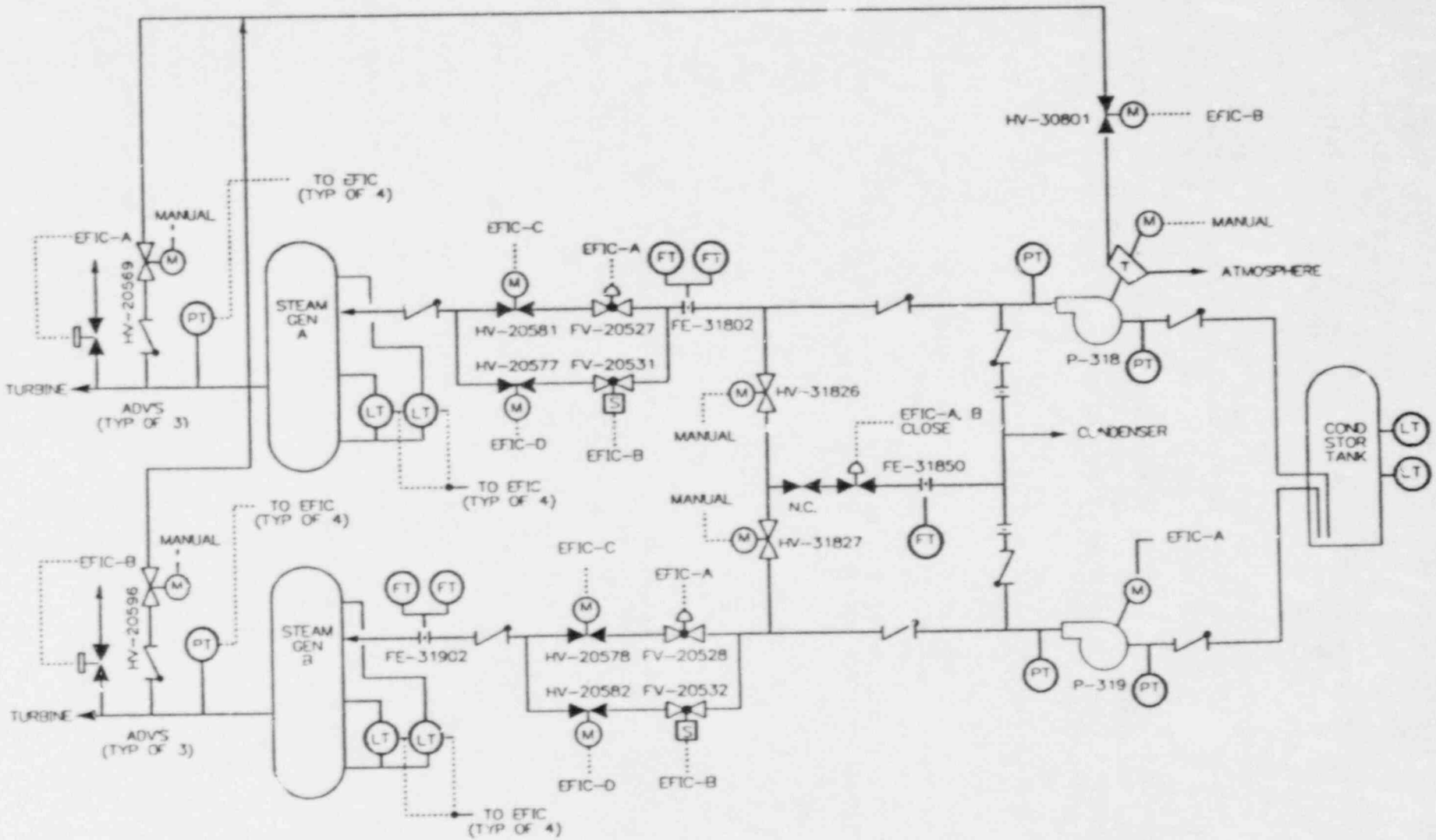


Figure 3.5 Rancho Seco auxiliary feedwater system flow diagram and EFIC system control (revised)

provides control of the atmospheric dump valves, and is used to isolate main feedwater (MFW) flow under certain conditions as discussed below. The following functions are accomplished by the EFIC system:

(1) monitoring of plant conditions and automatic initiation of AFW flow to both OTSGs when required (manual initiation capability for AFW is also provided)

(2) automatic control of AFW flow rate to achieve and maintain proper OTSG levels, in accordance with established setpoints, to minimize overcooling and undercooling of the primary system (manual control capability for AFW is also provided)

(3) automatic isolation of AFW and MFW flow to a depressurized (ruptured) OTSG

(4) automatic control of the atmospheric dump valves (ADVs) independent of the ICS (manual control capability for the ADVs is also provided)

(5) automatic closure of the MFW isolation valves upon detection of high OTSG water level to prevent an OTSG overfill condition

The EFIC system consists of four physically separate and electrically independent channels: A, B, C, and D. These channels are powered from Class 1E battery-backed emergency buses S1A2-1, S1B2-1, S1C2-1 and S1D2-1 respectively. The EFIC system instrument channels, logic and control circuitry, and actuated/controlled equipment used to initiate and control AFW flow are powered from Class 1E diesel generator-backed or battery-backed buses that are separate from the buses providing power to the ICS and non-nuclear instrumentation (NNI) system. The EFIC system controls and indications are located on control console H1SS(E) in the main control room. The EFIC system logic and actuation circuitry is located within four cabinets (one cabinet for each EFIC channel) located in the nuclear service electrical building (NSEB). Certain EFIC-system-controlled equipment receives actuation/control signals directly from these cabinets (e.g., AFW flow control valves and ADVs). Other EFIC-system-controlled equipment receives actuation/isolation signals from the EFIC logic via trip interface equipment (TIE) cabinets (e.g., MFW flow control and isolation valves, and AFW system pumps). The TIE cabinet circuitry interfaces between the EFIC system actuation logic and field equipment. Four TIE cabinets are provided in the NSEB. For each train of EFIC-system-actuated equipment, one cabinet is used to interface between the EFIC system and Class 1E circuits, and another links the EFIC system and non-Class 1E circuits.

Each EFIC channel receives analogue inputs from steam generator level and steamline pressure transmitters associated with each OTSG. The level signals are density compensated to provide an accurate indication of actual water level. The EFIC system also receives initiation signals from the reactor protection system (RPS) and the safety features actuation system (SFAS). During plant operation, the EFIC system constantly monitors the input signals, and generates individual channel level protective action signals whenever process parameters exceed their preestablished setpoint values. Actual system-level actuation will take place only if at least two of the four EFIC instrument channels have initiated commands for protective action.

Revised Figures 3.6, 3.7, 3.8, and 3.9 illustrate the input and output signals associated with EFIC channels A, B, C, and D, respectively. The EFIC system logic is subdivided into the following logic functions:

(1)	Input logic	Receives and provides individual channel-level trip and bypass signals to the remaining portions of the EFIC system logic
(2)	Actuation logic	Initiates AFW system flow to the OTSGs
(3)	Control logic	Controls AFW system flowrate and OTSG level (this logic also includes the ADV controls)
(4)	Vector logic	Isolates AFW system flow to a depressurized OTSG and
(5)	Isolation logic	Isolates MFW system flow to a depressurized OTSG or to an OTSG with a high-high water level

Figure 3.10 is an overall block diagram of the EFIC system that shows the EFIC logic functions and the associated actuated equipment. The EFIC system and its actuated/controlled equipment will be completely installed, tested, and fully operational at restart as governed by the Rancho Seco Plant Technical Specifications.

EFIC System Initiation of AFW

The EFIC system is designed to initiate AFW (1) on low water level in either OTSG ($\geq$9 inches), (2) on low pressure in either OTSG steamline, ($\geq$575 psig), (3) when all four reactor coolant pumps trip (this signal is provided to the EFIC system from the RPS), (4) on the loss of both MFW pumps at more than 20% reactor power (this is an anticipatory trip signal also provided to the EFIC system from the RPS), and (5) on reactor building high pressure (<4 psig), or (6) on reactor coolant system (RCS) low pressure (>1600 psig). The EFIC system receives the reactor building high pressure and RCS low pressure signals from the SFAS.

The EFIC system AFW actuation logic is arranged in a 1-out-of-2-taken-twice logic configuration. All four EFIC input logic channels provide AFW initiation commands to the AFW actuation logic modules that are physically located in the A and B EFIC channel cabinets. The EFIC system AFW system actuation logic is functionally shown in revised Figure 3.11. Actuation of AFW pump P-319 and the associated train A control valves occurs when the actuation logic modules in the A EFIC channel cabinet receive channel level initiate commands from EFIC system input logic channels A or B and C or D. AFW pump P-318 and the associated train B control valves are actuated when the actuation logic modules in the B EFIC channel cabinet receive "initiate" commands from EFIC system input logic channels A or C and B or D. Because all four EFIC channels monitor the same parameters, they should all simultaneously issue "initiate" commands, thereby actuating both AFW system trains. The channel level AFWS actuation signals are not "sealed-in" by the input logic circuitry of the EFIC system. However, once the 1-out-of-2-taken-twice actuation logic is satisfied, the system (train) level actuation signal is sealed in and cannot be reset until the initiating condition has returned to normal and the actuation logic reset

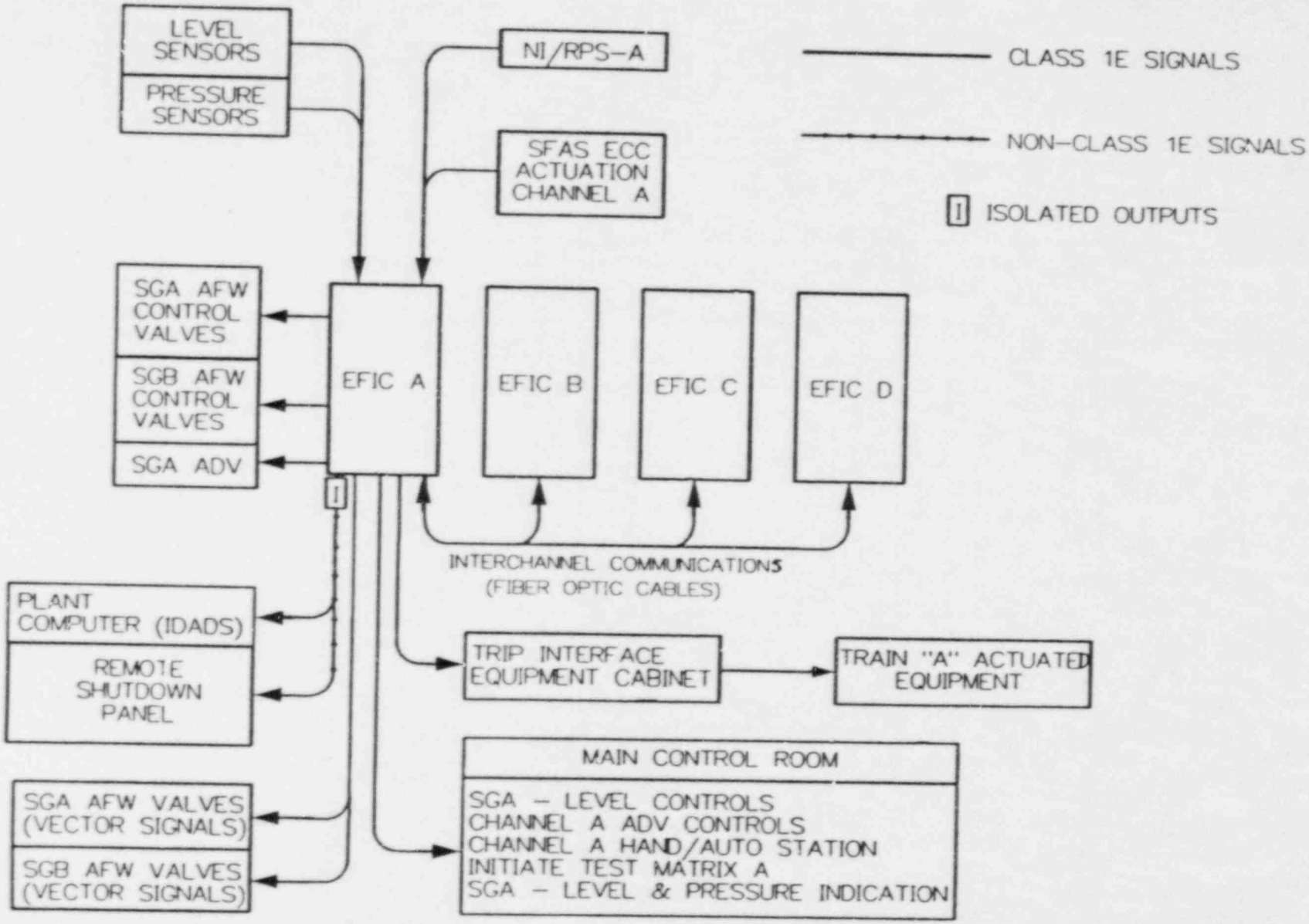


Figure 3.6 EFIC channel A (revised)

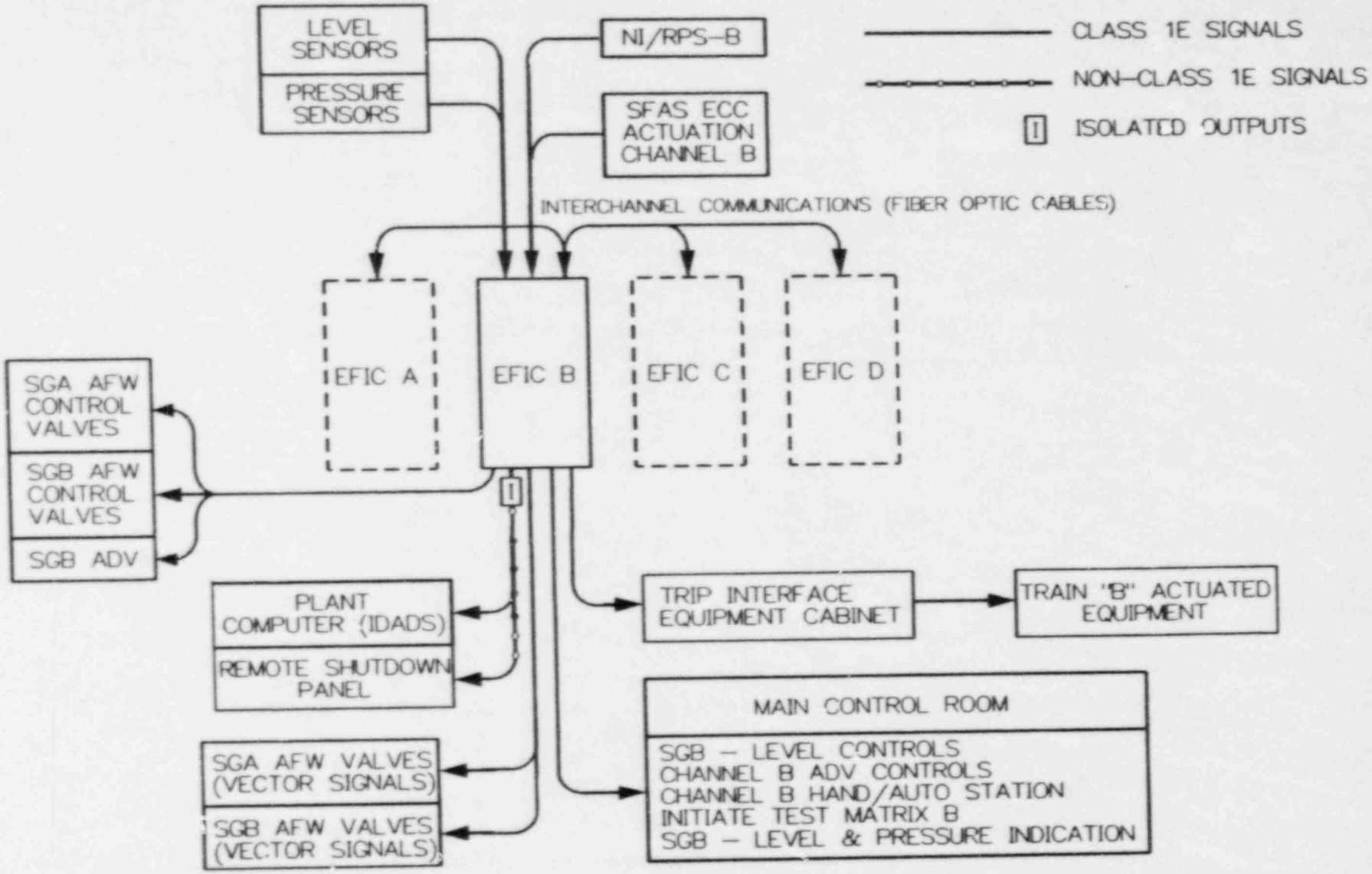


Figure 3.7 EFIC channel B (revised)

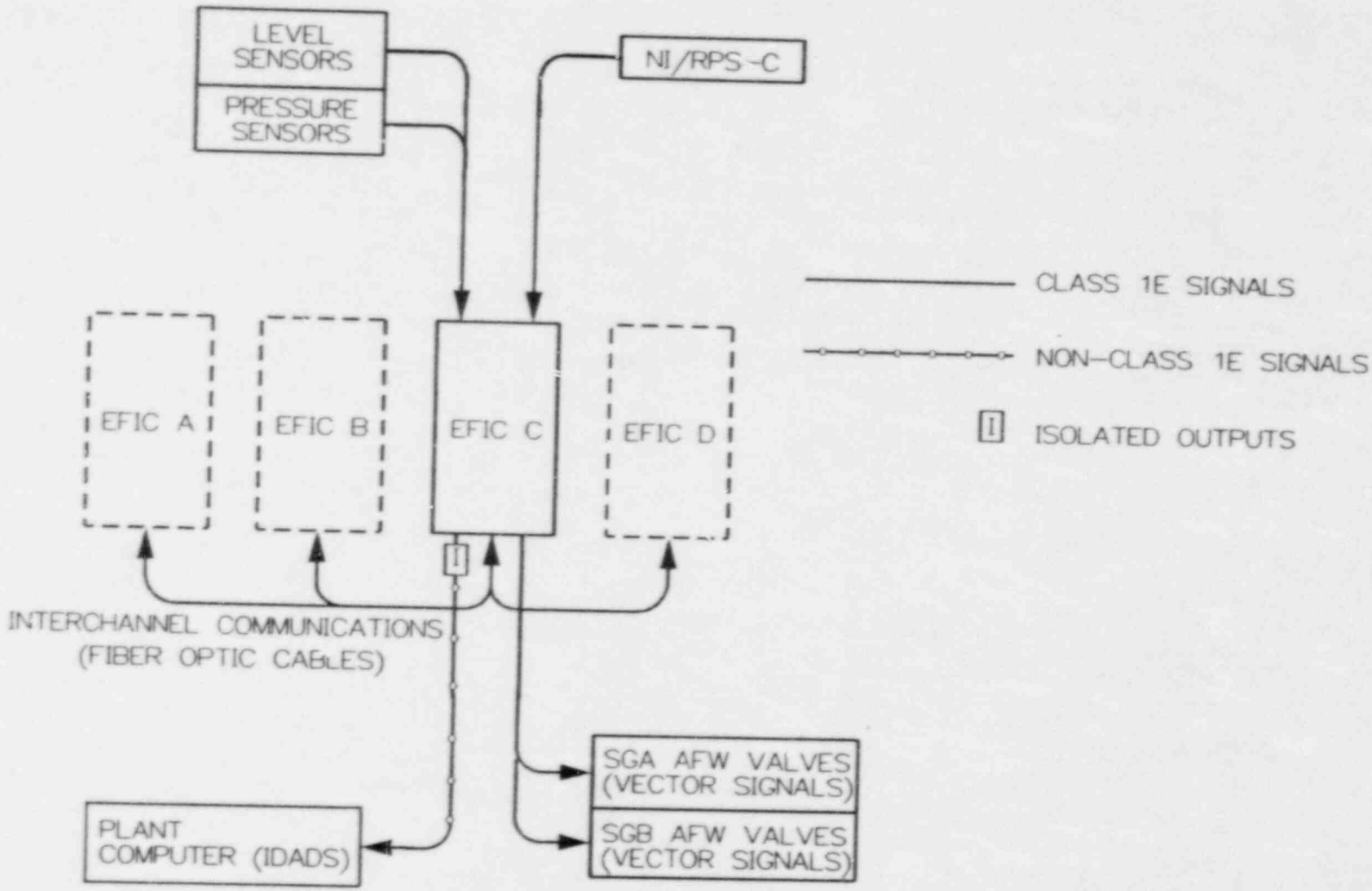


Figure 3.8 EFIC channel C (revised)

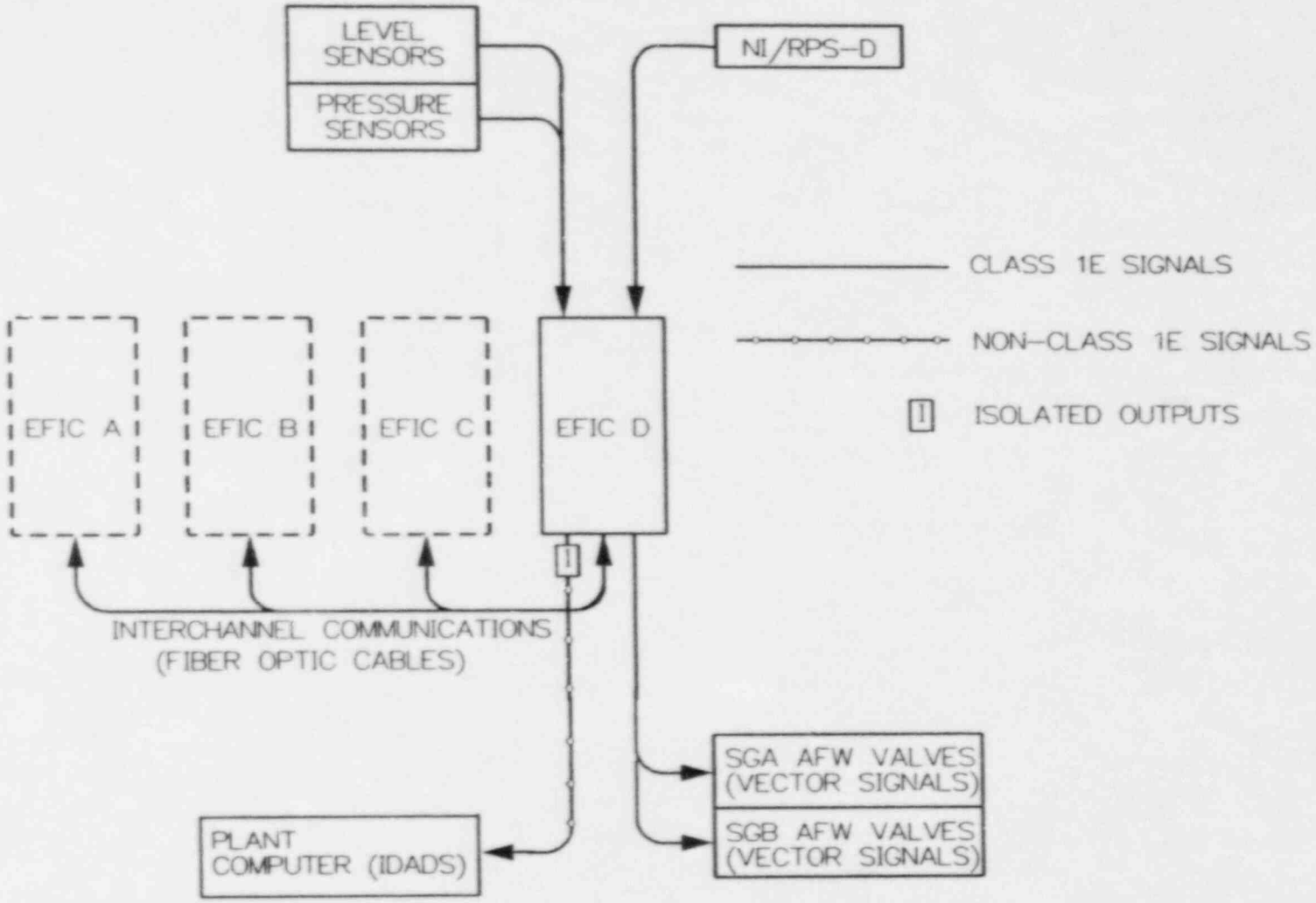


Figure 3.9 EFIC channel D (revised)

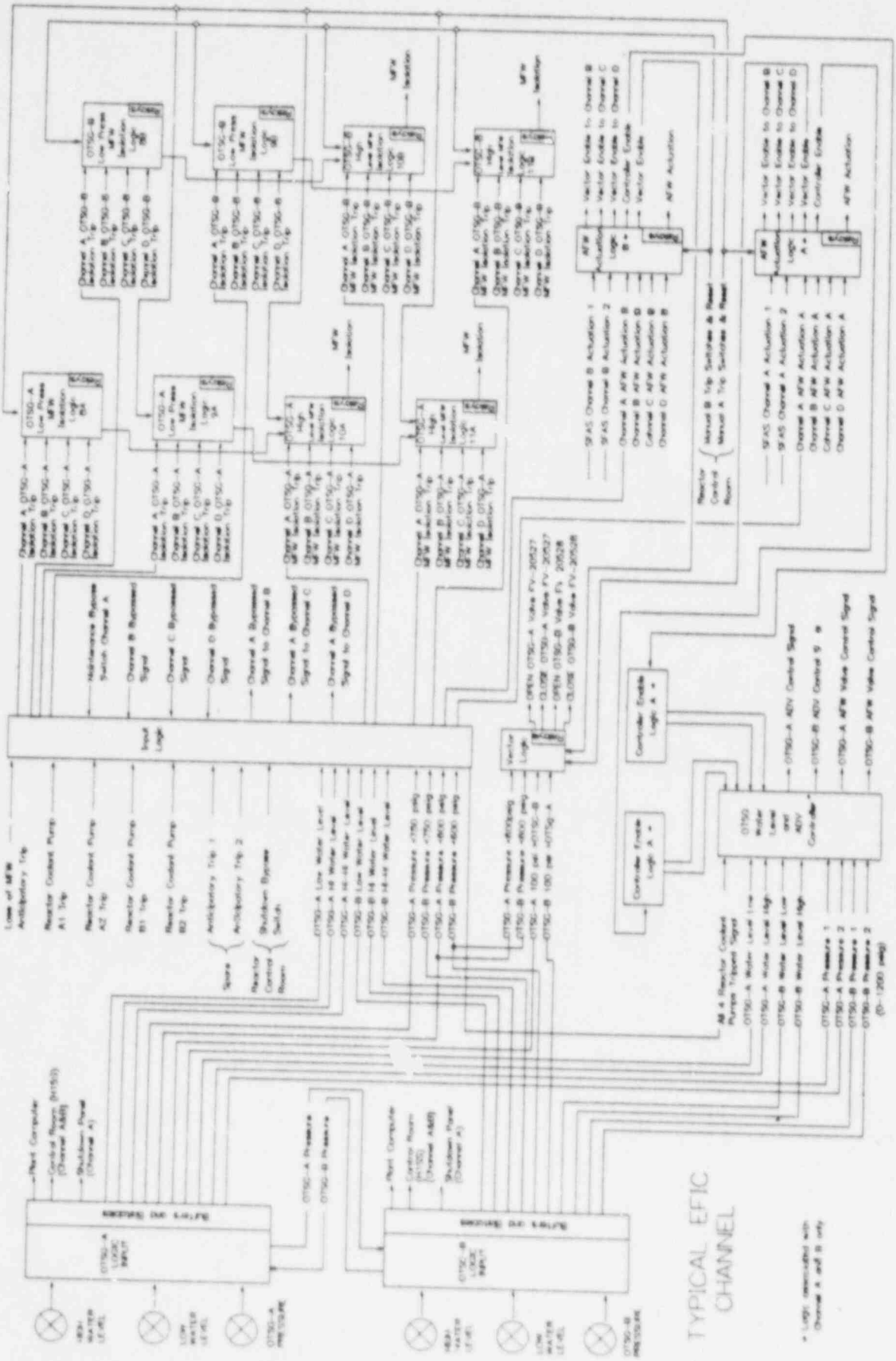


Figure 3.10 Typical EFIC channel

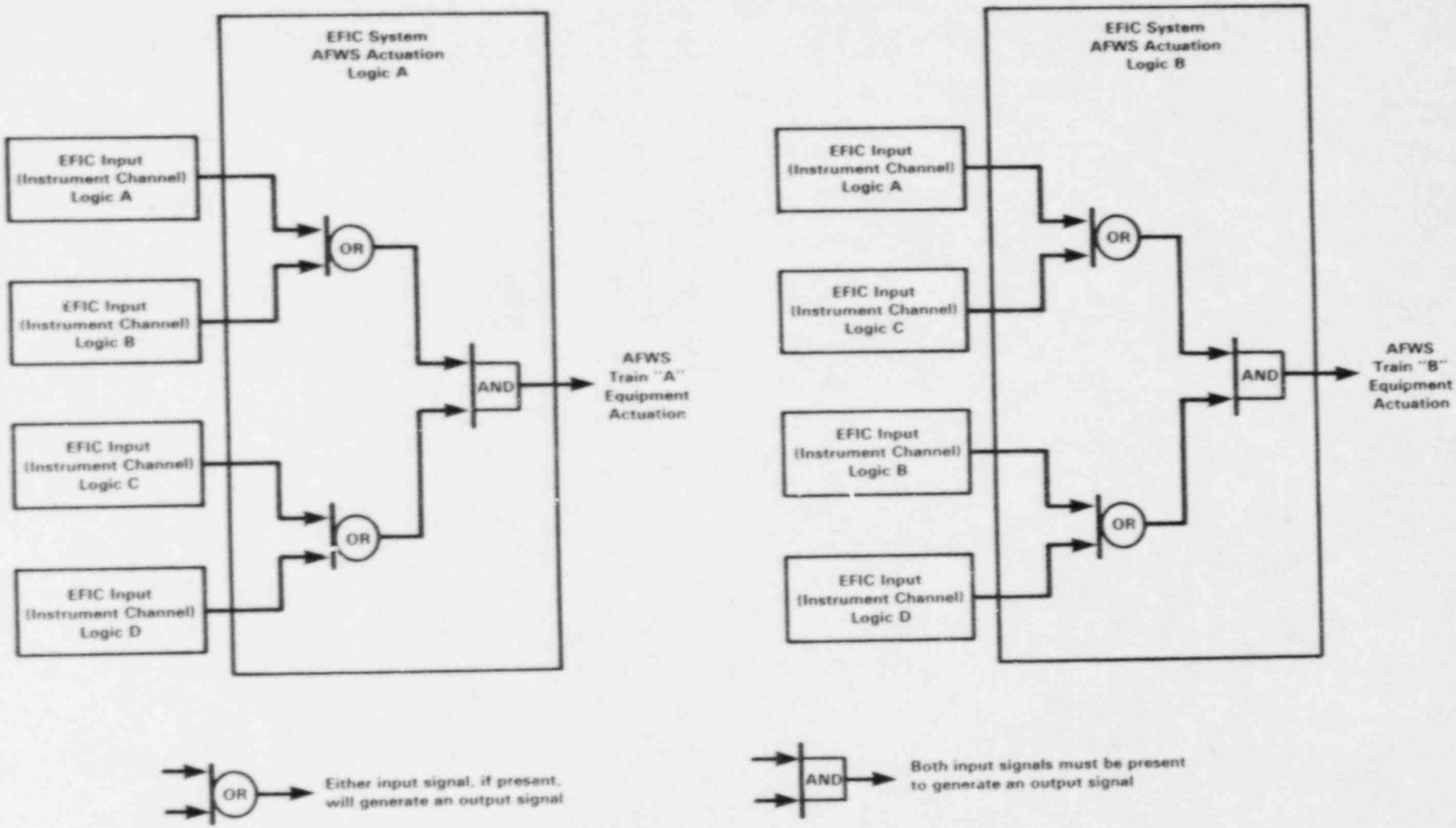


Figure 3.11 EFIC system initiation of auxiliary feedwater (revised)

pushbutton is depressed. The actuation logic seal-in circuits ensure that completion of the associated protective actions occurs upon generation of a system level actuation signal.

EFIC System Isolation of Main Feedwater

Before the December 26, 1985 event, the Rancho Seco plant used a non-safety related main steamline failure logic (MSLFL) system to isolate MFW flow to the OTSGs in the event of a failure of a main steamline (MSL). MFW was isolated by the automatic closure of three valves in each feedwater line: the main flow control valve, the downstream series MFW stop valve, and a single startup MFW flow control valve located in a parallel line around the other two valves. In NUREG-1195, the following concerns about the MSLFL system were identified: (1) the valve arrangement does not appear to meet the single-failure criterion with respect to MFW system isolation, (2) the MSLFL system is not a safety-related system but is used to perform a safety-related function, and (3) the MFW system flow control valves might not be adequate for isolation.

The MSLFL system detected low steamline pressure (indicative of an MSL break) via pressure switches on the steam header downstream of each OTSG. Two redundant MSLFL system trains consisting of sensing elements, dc-powered logic, and actuation devices were provided. Two pressure switches within each train were configured in a 2-out-of-2, energize-to-actuate, logic arrangement. When the logic was satisfied, solenoid-operated valves would actuate to block the control air to, and vent the air from, the MFW system flow control valves, causing them to close. The ICS would then, in turn, close the MFW stop valves. The ICS is designed to close the stop valves when the main flow control valves go to less then 20% open. The Rancho Seco Final Safety Analysis Report (FSAR) analysis assumes the successful operation of the non-safety-related MSFLS and the non-safety-related ICS to close the MFW stop valves for a main steamline break accident.

Since the December 26, 1985 event, the licensee has modified the MFW system valve configuration. An additional motor-operated isolation valve has been installed in the MFW flow path to each OTSG downstream of the flow control and stop valves, as shown in Figure 3.12. The non-safety-related MSLFL system has been removed and the MFW isolation function will now be performed by the safety-related EFIC system. The EFIC system will isolate the MFW flow control and block valves, and the new isolation valves. During normal operation, the ICS still provides control of the MFW flow control and block valves.

The EFIC system will isolate MFW flow to an OTSG when either a pressure of less than 600 psig or a high water level is detected in that OTSG. Four redundant instrument channels, A, B, C, and D, are provided to monitor each of these parameters for each OTSG. The EFIC system MFW isolation logic is arranged in a 1-out-of-2-taken-twice logic (identical to the AFW system actuation logic) and is shown in Figure 3.13. MFW isolation to an OTSG occurs when the logic modules in EFIC system cabinet A receive commands from input logic Channels A or B and C or D, or when the logic modules in EFIC system cabinet B receive "initiate" commands from logic Channels A or C and B or D.

The EFIC system's MFW isolation logic for channel A cabinet isolates MFW valves FV-20525, FV-20529 and FV-20575 to OTSG A, and valves FV-20526, FV-20530, and

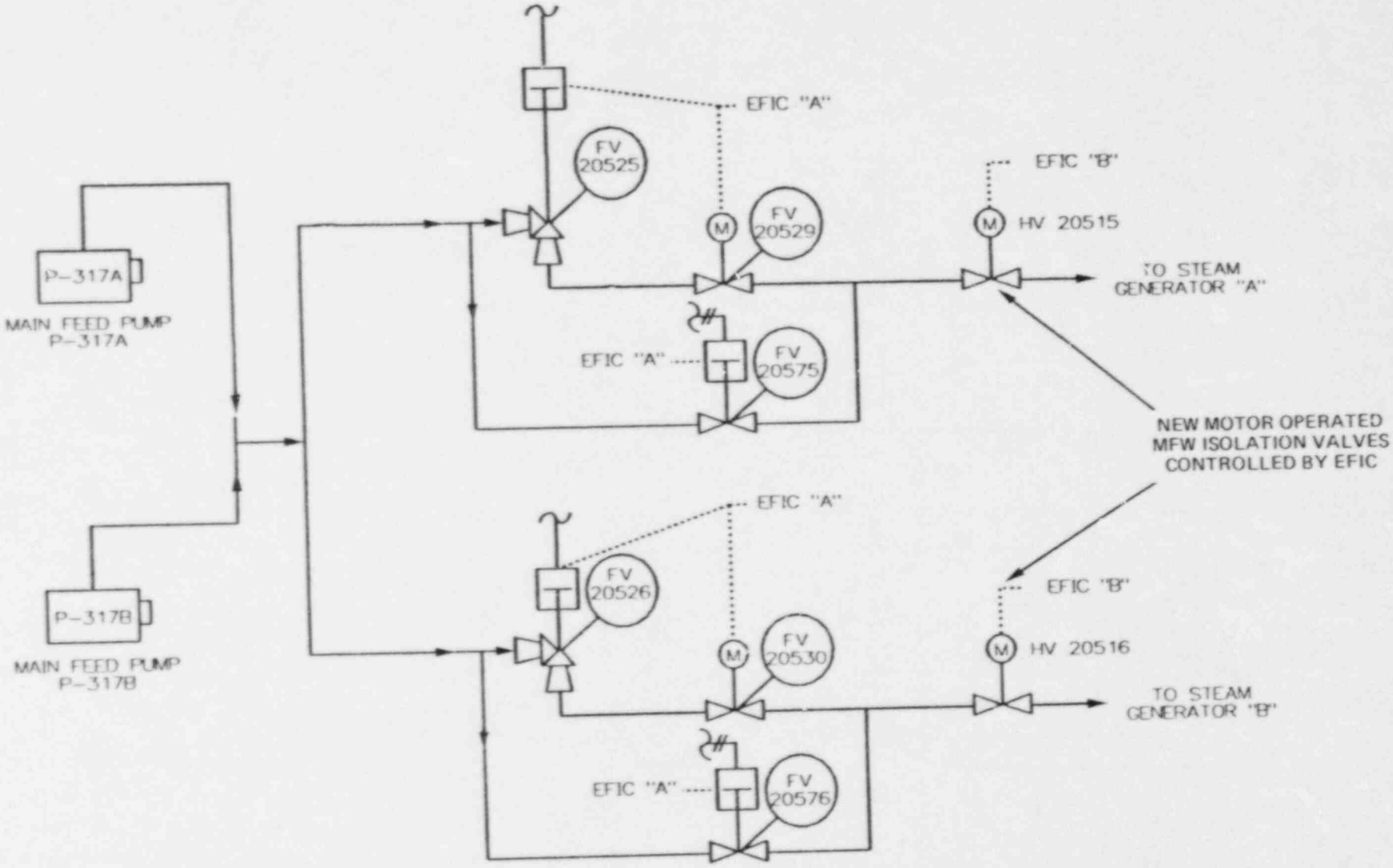


Figure 3.12 Main feedwater system

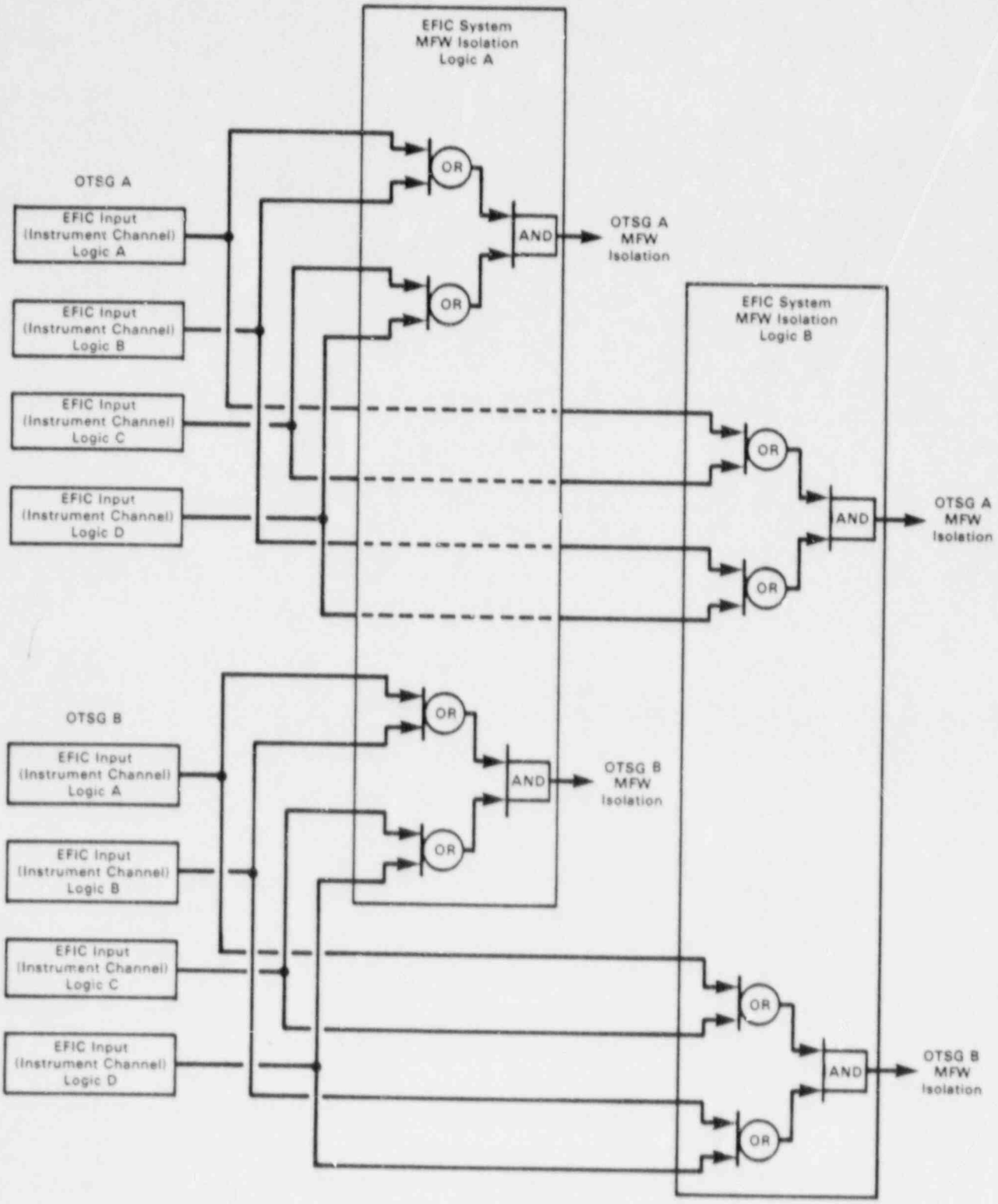


Figure 3.13 EFIC system isolation of main feedwater

FV-20576 to OTSG B. The EFIC system's MFW isolation logic for channel B cabinet isolates valve HV-20515 in the MFW line to OTSG A and valve HV-20516 in the MFW line to OTSG B. Because all four EFIC system input logic (sensing) channels monitor the same parameters, they should simultaneously issue commands causing all valves used for MFW isolation to an OTSG to close.

Valves FV-20525, FV-20575, FV-20526, and FV-20576 are air-operated MFW flow control valves MFW stop valves FV-20529 and FV-20530 are powered from 480-V motor control center (MCC) S2A3 and are backed up by diesel generator GEA2. The new downstream series isolation valves (HV-20515 and HV-20516) are powered from 480-V MCC S2B3, and are backed up by diesel generator GEB2.

On the basis of the review of the information provided by the licensee concerning modifications to provide additional MFW system isolation valves, and to initiate isolation of the new and existing valves by the safety related EFIC system, the staff concludes that the MFW isolation function conforms to the single failure criterion of IEEE Standard 279-1971. Therefore, the staff concludes that the concerns of NUREG-1195 in this area have been resolved.

EFIC System Isolation of AFW

The EFIC system includes logic used to isolate AFW flow to a ruptured or depressurized OTSG. This logic is referred to as the "feed-only-good-generator" (FOGG) or "vector" logic. Upon actuation, the vector logic precludes the continued addition of AFW to a depressurized OTSG, thus minimizing the overcooling effects of a steam leak. The vector logic may isolate AFW to one OTSG only; never to both.

Each EFIC system channel contains vector logic. Each set of vector logic receives OTSG pressure signals from each of the four EFIC system channel input logics. The pressure information received is (1) OTSG A pressure less than 600 psig, (2) OTSG B pressure less than 600 psig, (3) OTSG A pressure 100 psig greater than OTSG B pressure, and (4) OTSG B pressure 100 psig greater than OTSG A pressure.

Each vector logic also receives a vector/control "enable" signal from both EFIC channel A and channel B upon AFW system actuation. The vector logic develops signals for open/close control of OTSG A and OTSG B AFW valves. The individual vector logics are not single-failure tolerant (i.e., a single failure could cause an inadvertent valve closure or could keep a valve from closing when required). However, the combination of four redundant and independent vector logics, and the AFW system flow control valve/isolation valve arrangement (i.e., two parallel flow paths for each OTSG, with two series valves in each path) ensures that any EFIC system single failure will neither prevent addition nor isolation of AFW to an OTSG when required. The vector logic outputs are in a neutral state until enabled by the control/vector enable from the channel A or B AFW actuation logics. When enabled, the channel A vector logic issues close commands to valves FV-20527 and FV-20528. The channel B vector logic issues close commands to valves FV-20531 and FV-20532. The channel C vector logic issues open or close commands to valves HV-20578 and HV-20581. The channel D vector logic issues open or close commands to valves HV-20577 and HV-20582. The table that follows shows the OTSG pressure conditions that cause the vector logic to isolate AFW flow.

Pressure status	OTSG A valves command	OTSG B valves command
If OTSG A & OTSG B > 600 psig	Open	Open
If OTSG A > 600 psig & OTSG B < 600 psig	Open	Close
If OTSG A < 600 psig & OTSG B > 600 psig	Close	Open
If OTSG A < 600 psig & OTSG B < 600 psig and OTSG A & OTSG B are within 100 psig	Open	Open
If OTSG A < 600 psig & OTSG B < 600 psig and OTSG A is 100 psig > OTSG B	Open	Close
If OTSG A < 600 psig & OTSG B < 600 psig and OTSG B is 100 psig > OTSG A	Close	Open

EFIC System OTSG Level Control

AFW to the OTSGs is controlled by logic contained within channels A and B of the EFIC system. The control logic becomes active when the EFIC system actuates AFW. The system is designed so that either channel will control water level in both OTSGs by controlling its own dedicated control valve for each AFW train. The EFIC system's control logic for channel A provides signals to air-operated valves FV-20527 (OSTG A) and FV-20528 (OTSG B) and the control logic for EFIC system channel B provides signals to solenoid-operated valves FV-20531 (OSTG A) and FV-20532 (OSTG B) for control of AFW flow. The duplication of control channels provides added assurance that sufficient AFW flow will be delivered to at least one OTSG to maintain water level. However, duplication of the control channels does not preclude the possibility of excessive AFW flow and consequent OTSG overfill. Operator intervention is relied on to prevent OTSG overfill. Flow-restricting venturis have been installed in the AFW system injection lines to reduce the AFW flow rate.

There are three different modes of automatic level control, depending on whether one or more reactor coolant pumps are running and whether the "ECC setpoint" has been selected for emergency core cooling (ECC). With one or more reactor coolant pumps operating, the EFIC system level control logic automatically controls OTSG level at a setpoint value of 27.5 inches. When none of the four reactor coolant pumps are running, the level controller automatically selects a setpoint of 317 inches, which is high enough to ensure good natural circulation. The third level setpoint of 381 inches (the ECC setpoint) is

manually selected if all four reactor coolant pumps are off and the plant is in a small-break loss-of-coolant-accident (LOCA) transient. The ECC setpoint is used to promote condensation heat transfer from the primary system.

The licensee has stated that the level control system is based on a design utilized in other B&W reactor plants, and is expected to provide stable, reliable level control of the water level in the OTSGs.

EFIC System Control of the Atmospheric Dump Valves

The EFIC system channel A and channel B control logic also provides control of the two trains of atmospheric dump valves (ADVs) for steamline overpressurization control. Atmospheric dump valves PV-20571 A, B, C and PV-20562 A, B, C are modulating control valves that relieve main steam to the atmosphere from main steamline A and main steamline B, respectively. EFIC system channel A will continuously monitor pressure in main steamline A and will signal PV-20571 A, B, and C to open if pressure in that line exceeds a setpoint value of 1020 psig. EFIC channel B will similarly control PV-20562 A, B, and C.

Before the December 26, 1985 event and subsequent installation of the EFIC system, the ADVs were powered and controlled by the non-safety-related integrated control system. The ADVs are now controlled by the safety-related EFIC system, which is electrically independent of the ICS.

Two of the three ADVs per steamline are normally blocked during reactor operation via upstream local manually operated valves. The unblocked ADV for each steamline has an associated upstream, normally open, remote, manually controlled, motor-operated valve that provides the operator with the ability to isolate a stuck-open ADV to prevent an uncontrolled steam release that could result in overcooling of the primary system. Although this valve is powered from the EFIC system buses, it can be operated independent of the EFIC system ADV control logic/circuitry. A single OTSG pressure transmitter is used to provide the input signal for each channel of ADV control logic. If an unblocked ADV fails to open, the downstream main steam safety valves (MSSVs) will open to relieve steam pressure, if steam pressure should increase to the MSSV open setpoints.

EFIC System Interfaces

The major systems that interface with the EFIC system are:

- auxiliary feedwater system
- main feedwater system
- main steam system
- once-through steam generator system
- electrical distribution system
- reactor protection system
- safety features actuation system
- interim data acquisition and display system
- safety parameter display system
- Appendix R remote shutdown panel (H2SD)
- plant instrument air system
- main control room panels/consoles (H1SS, H1RC, H2YS, and H2SF)

To ensure proper isolation between the Class 1E EFIC system and non-Class 1E systems with which it interrelates, the EFIC system design utilizes fiber optic cables, optical isolators, and isolation relays.

The following table lists the non-Class 1E interface systems and the specific type of isolation used to prevent faults within the non-Class 1E systems from degrading the EFIC system safety functions. The staff concludes that the isolation provided between the EFIC system and non-safety-related systems is acceptable.

EFIC interface	Method of isolation
Auxiliary shutdown panel	· GE-SMB isolation switch · Optical isolators
Internal data acquisition and display system (IDADS) panel	Optical isolators
EFIC channel A and B with AFW valves	Isolation relays
All others	Fiber optics

EFIC System Bypasses

The EFIC system design includes two types of bypasses: maintenance bypasses and shutdown bypasses. The bypass circuitry is contained in the input logic portions of EFIC channels A, B, C, and D.

The maintenance bypass circuit design provides individual EFIC system input logic channel bypass capability for each of the four channels. The EFIC system is designed to allow channel testing from the input terminals to the actuated device controllers without placing the channel in maintenance bypass. Placing an EFIC system channel in maintenance bypass inhibits/disables the ability of that channel to perform its associated protective function. Maintenance bypasses are used to allow maintenance/repair of an inoperable channel during reactor operation without causing an unwanted/unnecessary channel trip. The use of EFIC system channel maintenance bypasses is controlled in accordance with plant Technical Specifications, where the inoperable/bypassed channels must be restored to an operable status within a specified time; or otherwise, reactor operation is suspended or restricted to power levels at which the associated protective action is no longer required. Channel bypass for maintenance is accomplished by placing the key-lock maintenance bypass switch at the associated EFIC system cabinet (in the NSEB) in the "MAINTENANCE BYPASS" position. Each EFIC channel key-operated maintenance bypass switch actuates an associated bypass status light at its local EFIC panel, and actuates an IDADS alarm in the control room to indicate when the maintenance bypass switch is being used. The indication associated with the IDADS alarm will be continuously displayed in the control room for as long as the bypass condition exists.

Interlock features within the EFIC system maintenance bypass circuitry make it impossible to bypass more than one channel at a time. These interlock features

ensure that the EFIC system is capable of performing its AFW actuation and MFW isolation safety functions, given a single failure when one channel is in maintenance bypass.

The EFIC system AFW actuation logic also receives maintenance bypass signals from the reactor protection system (RPS). Placing an RPS channel in bypass disables the RPS input signal to the corresponding EFIC system channel. An interlock feature is provided within the EFIC system channel input logic that will only allow the corresponding EFIC system channel to be bypassed when a RPS channel is bypassed. For example, if channel A of the RPS is placed in maintenance bypass, only a channel A EFIC system maintenance bypass can be actuated, and EFIC channels B, C, and D are automatically prevented from being placed in maintenance bypass. Should either EFIC channels B, C, or D be in maintenance bypass when EFIC channel A receives the RPS maintenance bypass signal, that EFIC channel will automatically be removed from bypass. Should a second RPS maintenance bypass signal be received by the EFIC system, all EFIC maintenance bypasses will be cleared/disabled (i.e., no EFIC system channel can be placed in maintenance bypass, and any EFIC system channel in maintenance bypass will automatically be removed from bypass).

To ensure that actuation/isolation does not occur during normal reactor shutdowns, the EFIC system shutdown bypass design provides the capability to defeat the AFW system automatic actuation logic and MFW isolation logic. The shutdown bypass logic is designed so that when the pressure in either OTSG drops below 725 psig, the reactor operator can manually initiate the shutdown bypass (before reaching the AFW actuation/MFW isolation setpoint value of 600 psig). A shutdown bypass cannot be initiated if the pressure in both OTSGs is greater than 725 psig.

Each of the four channels of EFIC system shutdown bypass logic can be actuated by one of two dedicated shutdown bypass switches. One shutdown bypass switch for each channel is located in the reactor control room on console H1SS(E), and the other shutdown bypass switch is located at the EFIC system channel cabinet. The shutdown bypass circuitry will "seal-in" following actuation. The seal-in can be removed by the shutdown bypass reset switch. The shutdown bypass will be automatically removed (restoring the EFIC system AFW actuation and MFW isolation protective functions) if the pressure in both OTSGs increases/returns to more than 725 psig i.e., if the permissive condition that allowed the bypass condition to exist is no longer satisfied). The shutdown bypass condition for each EFIC system channel is continuously indicated in the main control room and at the EFIC system cabinets in the NSEB for as long as the bypass condition exists.

3.1.3.2 Conformance to the Requirements of NUREG-0737, Item II.E.1.2

The EFIC design has been evaluated for its conformance to NUREG-0737, "Clarification of TMI Action Plan Requirements," Item II.E.1.2, "Auxiliary Feedwater System Automatic Initiation and Flow Indication." The requirements of NUREG-0737, Item II.E.1.2 can be met by providing a design for automatic AFW system actuation that meets the requirements of IEEE Standard 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." IEEE Standard 279 includes requirements regarding quality of components, compliance with the single-failure criterion, independence of redundant channels, control and protection

system interaction, channel/system bypasses, automatic and manual initiation, test capability, and system status information provided to the control room operator.

The automatic initiation circuits of the EFIC system are diverse, redundant, physically separated, electrically independent, and powered from battery-backed emergency buses. The two AFW pumps have diverse sources of motive power (electric motor and steam turbine). AFW system pump P-319 is actuated by EFIC channel A. The steam supply to the turbine-driven pump (P-318) is initiated by EFIC channel B. The failure of either channel A or B may cause one of the two AFW pumps to be unresponsive to an AFW actuation signal. However, one operational pump is sufficient to supply the water requirements of the system.

The EFIC and AFW systems are capable of providing sufficient AFW flow to the intact (pressurized) OTSG following a main steamline/main feedwater line break coincident with a loss of offsite power and a worst-case/most-limiting single failure as discussed below. Upon rupture of OTSG B (upstream of the turbine throttle and control valves or downstream of the main feedwater isolation valve and associated check valve), an AFW system actuation signal is initiated by the EFIC system logic which sends start signals to the AFW pump P-318 turbine and the AFW pump P-319 motor. MFW flow to the failed OTSG will be isolated by the EFIC system isolation logic shown in Figure 3.13. MFW isolation on OTSG low pressure will occur given any single failure within the EFIC system isolation logic or the MFW system isolation valves.

Assuming a loss of offsite power in conjunction with the rupture of OTSG B, emergency diesel generators GEA2 and GEB2 will receive start signals and provide emergency AC power to vital bus 4A2 and vital bus 4B2, respectively.

The following automatic and manual actions will occur or be available after the most limiting active single failures.

- If AFW pump/turbine P-318 fails, AFW pump/motor P-319, which receives a simultaneous EFIC start signal, will automatically supply AFW to OTSG A through the cross-connect line. The operator can also manually start the motor for AFW pump P-318 and supply AFW to OTSG A.

- If the motor for AFW pump P-318 fails, there would be no direct impact because the AFW pump P-318 turbine and the AFW pump P-319 motor receive simultaneous EFIC start signals, and both would supply water to OTSG A automatically.

- If one of the active valves in the AFW flow path to OTSG A fails and blocks the flow, the active valve in the redundant parallel flow path, which is controlled by a redundant EFIC system channel, will open and allow water to flow to OTSG A from both AFW pumps P-318 and P-319.

- If AFW pump/motor P-319 fails, the turbine for AFW pump P-318, which receives a simultaneous EFIC start signal, will automatically supply water to OTSG A.

- If one of the valves in the AFW flow paths to OTSG B fails to close to isolate flow, there would be no consequences because its series isolation

valve, controlled by a redundant EFIC system channel and powered from a separate vital bus, would close to isolate AFW flow to depressurized OTSG B.

- If EDG GEA2 and/or associated vital bus S4A fail, the AFW pump P-318 turbine will receive an EFIC start signal and will supply water to OTSG A via valves controlled by EFIC system channel B, and powered from EDG GEB2 and/or vital bus S4B.

- If EDG GEB2 and/or associated vital bus S4B fail, the AFW pump P-319 motor will receive an EFIC "start" signal and will supply water to OTSG A via the AFW cross-connect lines and valves controlled by EFIC system channel A and powered from EDG GEA2 and/or vital bus S4A. In addition, the AFW pump P-318 turbine, which receives a simultaneous EFIC start signal, will supply water to OTSG A.

The discussion above, which applies to the rupture of OTSG B, is applicable to the rupture of OTSG A.

When the AFW system is actuated, the four-channel EFIC AFW actuation system effectively becomes a two-channel system for OTSG water level control. Each of the two AFW trains has redundant valves to control the level in the OTSGs, and each of the redundant level control valves in a train is controlled by a different EFIC system control channel (A or B). Therefore, sufficient AFW flow to both OTSGs is ensured, given a single failure of any AFW flow control valve or its control circuitry.

The AFW system level control valves and the associated EFIC system control circuitry are designed to ensure that sufficient AFW flow is supplied to the OTSGs following a single failure (i.e., the AFW flow control valves fail open on a loss of control air or loss of motive power). However, because of this design, a single failure could lead to excessive AFW flow and subsequent OTSG overfill. The licensee considers this design characteristic to be acceptable based on the assumption that, although a failed open valve may result in overfilling, the rate of increase in OTSG level via AFW is slow, and that sufficient time exists for operator intervention. Although the B&W-designed EFIC system includes circuitry to prevent OTSG overfill via the AFW system, the licensee has elected not to use this feature. The licensee's basis for not allowing the EFIC system to isolate AFW flow on OTSG high level is that the EFIC system also isolates MFW to the OTSGs. Therefore, a common-mode failure could result in EFIC system isolation of both MFW and AFW flow to the OTSGs. It was, therefore, decided to only allow the EFIC system to isolate MFW. OTSG overfill protection for an AFW overfill event will be via high level alarms on the IDADS, and remote manual isolation via the AFW system control and isolation valves.

Two of the level control valves (one in each AFW train) are pneumatically operated (FV-20527 and FV-20528). The air supply for these valves is the plant air system, which is classified as a non-safety-related system. To ensure operation of these valves, a 2-hour, seismic Class 1, backup air supply has been provided for each valve train. The backup air supply will function only if the normal air supply is unavailable. This arrangement is considered acceptable. The instrument air system is further discussed in Section 3.1.2.4 ("Loss of Instrument Air to ICS/NNI System Components") of this report.

The EFIC system consists of four redundant channels of safety related circuits. Section 4.6, "Channel Independence," of IEEE Standard 279 states that channels providing signals for the same protective function shall be independent and physically separated to accomplish decoupling of effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction. Regulatory Guide 1.75, "Physical Independence of Electric Systems," references IEEE Standard 384-1974, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," which sets forth criteria for the physical separation of redundant safety related circuits and equipment.

All instrument/sensing channels providing inputs to the EFIC system are dedicated to one of four redundant input logic channels. The redundant instrument and input logic channels are physically separated and electrically independent from each other. All communications between redundant EFIC system channels (e.g., channel bypass status information) are accomplished via fiber optic cables.

The staff performed on onsite review of the physical separation provided between redundant Class 1E EFIC circuits, and between Class 1E EFIC circuits and non-Class 1E circuits, to determine if the installed design conforms to the separation criteria identified in Sections 5.6 ("Control Switchboards") and 5.7 ("Instrumentation Cabinets") of IEEE Standard 384. Where physical separation by enclosures is not possible because of the plant design, either a barrier or a 6-inch minimum separation distance should be provided. In those cases in which a barrier or 6-inch separation is not provided, the design must be analyzed to ensure compliance with Regulatory Guide 1.75 and IEEE Standard 384.

Compliance with the channel independence requirements of Regulatory Guide (RG) 1.75 is addressed by the licensee in engineering report ERPT-E0220, "Report on Conformance of NSEB and DG Building Electric Installation to RG 1.75," dated June 10, 1987. ERPT-E0220 addresses IEEE Standard 384-1974 as applicable to Rancho Seco and includes a discussion on how the specific requirements are met. The staff's evaluation and conclusions concerning ERPT-E0220 are detailed in the "Staff Evaluation by the Office of Nuclear Reactor Regulation of SMUD Approach to Compliance with RG 1.75 for New Diesel Generator Installation at Rancho Seco." This report specifically addresses: equipment separation, raceway separation, separation between redundant Class 1E raceways, wiring separation within enclosures, and raceway/circuit identification. The staff's onsite review of the physical separation provided between redundant Class 1E EFIC circuits, and between Class 1E EFIC circuits and non-Class 1E circuits confirmed that the installation at Rancho Seco was as described in ERPT-E0220. On the basis of review of ERPT-E0220, the staff concludes that the licensee's approach to demonstrating overall compliance with RG 1.75 requirements is acceptable. This issue is further discussed in Section 4.7.3 ("Class 1E Electrical Systems Associated With the Diesel Generators") of this report.

The information available in the control room for the operators to assess EFIC system status/performance is provided by the interim data acquisition and display system (IDADS), and instruments located on the EFIC system control console H1SS(E). The IDADS is a plant process computer system that monitors

plant conditions and performs various calculations, as well as trending, alarm, and post-transient data logging functions. Essentially all EFIC system status alarms are provided by the IDADS. The IDADS is a non-safety-related system, and is isolated from the safety-related EFIC system via an Anatec remote multiplexer system discussed in Section 3.1.3 of this report. The IDADS interface with the operators is two cathode-ray tube (CRT) displays located in the primary operating area of the control room. IDADS displays are also provided in the technical support center (TSC). Each IDADS alarm must be acknowledged by the operator, the condition that initiated the alarm must return to normal, and the IDADS alarm display must be "reset" in order for the alarm condition to clear. This design is similar to that of the control room main annunciators. During normal plant operation, each IDADS alarm condition sounds a bell, which is distinguishable from the main annunciator horn, and each alarm condition is logged by a printer in the control room. During a plant event (defined as a plant condition involving a reactor trip, SFAS actuation, EFIC system actuation, loss of offsite power, or main turbine trip), the IDADS alarm bell is suppressed for "non-critical" alarms; however, all alarm conditions will continue to be printed out in sequence. The IDADS includes a "plant event alarm summary" display (modeled after the main annunciator panels) that is automatically provided to the operators whenever a "critical" plant event alarm condition occurs (e.g., EFIC system actuation/isolation). The plant event alarm summary display is considered to be of equal importance to the main annunciators. The IDADS displays use white to signify a normal plant condition, reverse magenta for alarm conditions, reverse yellow upon operator acknowledgement, and blinking white upon return to normal. The human factors aspects of the IDADS will be evaluated as part of the detailed control room design review (DCRDR) to be completed after plant restart. The EFIC system status alarms provided by the IDADS include:

- AFWS actuation
- MFWS isolation
- loss of reactor coolant pump(s)
- approach to trip on OTSG high/low level, and OTSG low pressure
- OTSG overfill
- OTSG low-level trip
- OTSG low-pressure trip
- AFW flow test valve open
- EFIC system power failures
- EFIC system channel in maintenance bypass or module withdrawn
- vector logic isolation of AFW
- transfer of EFIC system control to the remote shutdown panel

In addition to the information provided by the IDADS, the reactor operator has status indicators for EFIC system parameters on control room panels H1SS(E), H1RI, H2YS, and H2SF, and local indications are provided on the EFIC system channel A, B, C, and D cabinets. Panel H1SS(E) provides the operator with the immediate information needed to determine the status of the EFIC system and the OTSGs should the IDADS be unavailable, and provides the operator with the means to manually initiate EFIC system safety functions. The following indications are provided on H1SS(E):

- OTSG A and B narrow-range level
- OTSG A and B wide-range level

- OTSG A and B pressure
- AFW pump P-318 and P-319 discharge pressure
- dual indication of AFW flow to OTSG A and B
- flow indication for the AFW test line

Controls are provided on H1SS(E) for manual operation of the AFWS pumps and valves. The operator has the capability to override EFIC control of the AFWS and assume manual control. Valve position indication is provided for the AFWS flow control valves, isolation valves, crosstie valves, and test valve. The circuits provided for manual initiation of AFW are so designed that (1) a single failure will not prevent manual initiation and (2) failure of the automatic initiation circuits will not preclude manual initiation and vice versa.

Each channel of the EFIC system is testable during plant operation. The testing features are designed to comply with Sections 4.9 ("Capability for Sensor Check") and 4.10 ("Capability for Test and Calibration") of IEEE Standard 279. The EFIC system circuitry can be tested during plant operation from the sensor outputs up to and including the trip actuation devices, without causing spurious actuations or preventing valid automatic actuation of the AFW system when required. The testing is accomplished by the use of pushbutton switches that initiate and reset a "half-trip" condition in the actuation circuitry for EFIC system-controlled equipment. The EFIC system includes "test results" circuit status lights that indicate a successful test upon proper operation of the actuation circuitry to achieve the half-trip condition. The process sensors providing inputs to the EFIC system will be calibrated while the plant is in cold shutdown. Instrument channel operability will be checked once per shift by comparing the indicated values (readouts) from redundant channels monitoring the same variables to ensure they are in agreement.

The periodic surveillance testing proposed by the licensee for the EFIC system is listed in Table 4.1-1, "Instrument Surveillance Requirements," of proposed Amendment 152, Revision 2, to the Rancho Seco plant Technical Specifications. The licensee transmitted the proposed amendment to NRC by letter GCA 87-263 dated July 31, 1987. Table 4.1-1 identifies the required frequencies for making instrumentation checks, tests, and calibrations. In general, EFIC system instrument channels are checked each shift, tested monthly, and calibrated at each refueling outage. The EFIC system AFW manual initiation circuits, automatic actuation logic and bypass circuitry are functionally tested each month. The MFW isolation and AFW valve control manual and automatic circuits (including vector signals) receive similar surveillance testing. The ADV control circuits are also tested monthly.

The staff reviewed the following preliminary EFIC system surveillance procedures (the final EFIC system surveillance procedures had not been completed by the licensee at the time of this review):

- SP 1, "Shift Surveillance and Instrument Check"
- SP 2, "Daily Instrument Checks and Systems Verification"
- SP 98, "Monthly Test of Auxiliary Feedwater Atmospheric Dump Valve Manual Controls"

- SP 99, "Refueling Interval Auxiliary Feedwater System Auto Start Test for EFIC Actuation"

- SP 495A, B, C, and D, "Monthly Test of EFIC Channel A (B, C, D) Pressure and Level Bistables and Bypasses"

- SP 496A and B, "Monthly Test of EFIC Channel A (B) Manual and Automatic Trip Logic, Steam Generator Level, and Pressure Controls"

- SP 498, "Monthly Test of EFIC Vector Logic"

- SP 499A, B, C, and D, "Refueling Interval Calibration of EFIC Channel A (B, C, D) Pressure Circuitry, Pressure Bistables and Time Delay Module"

The preliminary procedures were reviewed to verify that (1) the scope of the tests is sufficient to fulfill the testing requirements identified in proposed Table 4.1-1 of the Rancho Seco Technical Specifications, (2) the tests provide such complete end-to-end overlap testing that the entire EFIC system is demonstrated to be operable, including coincident logic and actuation devices, (3) all EFIC system input signals are tested, including those provided by the RPS and SFAS, and (4) operability of EFIC system control room indications provided to the operators are included in the tests. On the basis of its review, the staff concludes that the above procedures, with the exception of SP1 and SP2, are adequate to perform the desired EFIC system testing as required by the Rancho Seco Technical Specifications, and therefore, are acceptable. However, the staff has not reviewed test procedures SP500A, B, C, and D for the EFIC system level circuitry, level bistables, and time-delay modules. The licensee has stated that these procedures are essentially identical to SP499A, B, C, and D, which were reviewed. Neither has the staff reviewed test procedures SP406A, B, C, and D or SP42A and B , which are used to verify operability of the RPS and SFAS interfaces with the EFIC system and the associated EFIC system circuits. Based on discussions with the licensee, these tests involve the initiation and subsequent reset of half-trip conditions similar to other EFIC system tests described above, and appear to be acceptable.

SP1 is the procedure used to fulfill Technical Specification requirements for EFIC system instrument channel checks performed each shift. SP1 does not include provisions for verifying operability of EFIC system indications (vertical indicators) for OTSG level and pressure displayed on control room panel H1SS(E). SP1 currently verifies instrument channel operability by comparing redundant input signals before operability is indicated. This type of channel check verifies operability of all four sensors by comparison of redundant input signals. However, the staff believes that SP1 should also require comparison of displayed values to detect failures that may have occurred in the indicators (or their input circuits) used by the control room operators (only two of the four channels are displayed). SP2 is used to verify operability of the EFIC system backup bottled air supplies by reading local pressure indications. SP2 does not specify what constitutes an acceptable pressure value (i.e., acceptance criteria are not provided), nor does SP2 include provisions to ensure that both redundant backup air supplies are checked. The licensee should revise SP1 and SP2 to resolve the above concerns.

The staff has reviewed the operability requirements for EFIC system instrumentation, the required limiting conditions for operation (LCOs) and associated

action statements for when operability requirements cannot be met, as listed in Table 3.5.1-1, "Instruments Operating Conditions," of the Rancho Seco Technical Specifications. In general, if one of the four EFIC system channels monitoring a parameter becomes inoperable, it must be restored to service within 7 days or the reactor is to be placed in at least hot shutdown within the next 12 hours. Although 7 days is longer than typically allowed by the Standard Technical Specifications, (STS) the staff considers 7 days to be acceptable because even with an inoperable channel, the EFIC system will perform its AFW initiation and MFW isolation functions, given a single failure. If a second EFIC system channel should become inoperable, one of the inoperable channels must be placed in trip, and one of the inoperable channels must be restored to service within 48 hours. If these conditions are not met, the reactor must be placed in at least hot shutdown within the next 12 hours. If more than two channels become inoperable, the reactor is to be brought to hot shutdown within 4 hours and to cold shutdown within the subsequent 12 hours.

If one of the EFIC system manual initiation circuits/channels or automatic actuation logics should become inoperable (these circuits consist of two channels/trains as opposed to the four channels used to monitor EFIC system initiating parameters), the inoperable channel must be restored to an operable status within 48 hours or the reactor is to be in at least hot shutdown within the next 12 hours. Should both channels ever be inoperable, the reactor is to be placed in hot shutdown within 4 hours and to be in cold shutdown within the next 12 hours. The 48-hour out-of-service time for one of these channels is consistent with EFIC system operability requirements at other B&W operating reactors, and with STS-allowed out-of-service times for engineered safety features (ESF) system equipment.

In order to allow routine periodic surveillance testing to demonstrate operability of EFIC system instrumentation without placing the plant in an LCO, an EFIC system instrument or logic channel may be removed from operation for a maximum of 6 hours, provided that the remaining redundant channels are operable.

On the basis of its review, the staff concludes that the Rancho Seco Technical Specification operability and surveillance requirements proposed for the EFIC system are acceptable for plant restart.

Conclusion

Based on the review of EFIC system design documents, electrical schematic/elementary diagrams, logic diagrams, proposed technical specification operability and surveillance requirements, additional system design information provided by the licensee, and an onsite review of the installed EFIC system, the staff concludes that the EFIC system complies with (1) the requirements of NUREG-0737, Item II.E.1.2 regarding safety-grade automatic initiation of the AFW system and (2) the criteria applicable to ESF systems identified in Section 7.3 of the Standard Review Plan (NUREG-0800) and, therefore, is acceptable for plant restart.

3.1.3.3 EFIC System Independence From the ICS/NNI System

TMI Action Plan Item II.K.2.2, "Control of Auxiliary Feedwater Independent of the Integrated Control System," requires that procedures and training for

initiation and control of AFW independent of the ICS must be provided for B&W-designed reactors.

The AFW system design installed at the time of the December 26, 1985 event consisted of redundant (parallel) flow paths to each OTSG with a single flow control valve (FCV) in each path. For each OTSG the FCV in one path was controlled by the ICS, and the FCV in the parallel flow path was controlled by the SFAS. The design basis for having both an ICS-operated FCV and a SFAS-operated FCV was to ensure that there would always be an available AFW flow path to each OTSG, given a single failure of an FCV. However, if a SFAS-operated FCV should fail, the only means of providing AFW to the associated OTSG would be via the non-safety-related ICS-operated FCV. Furthermore, assuming that an AFWS pump is running, to isolate AFW flow to an OTSG would require successful operation of both the SFAS-operated FCV and the non-safety-related ICS-operated FCV. The FCV controlled by the failed ICS could not be closed during the December 26, 1985 event; this led to OTSG overfill and significant overcooling of the primary system.

The newly designed/upgraded AFW system and safety-related EFIC system do not have any interface with the non-safety related ICS. The EFIC system provides redundant safety-related capability to initiate and isolate AFW flow to each OTSG as discussed in Section 3.1.3.1 ("EFIC System Design and Operation") of this report. Section 7.2.3 of NUREG-1195, "Loss of Integrated Control System Power and Overcooling Transient at Rancho Seco on December 26, 1985," states that had the EFIC system been installed, the overcooling event would have been much less severe, and probably would not have exceeded technical specification limits.

On the basis of the review of the EFIC system design for initiation and control of the AFWS independent of the ICS and NNI system, the staff concludes that the Rancho Seco design conforms to the requirements of NUREG-0737, Item II.K.2.2, and is acceptable for plant restart.

3.1.4 Main Feedwater System Response to ICS/NNI System Failures

This issue is discussed in Section 3.1.2.6, "Loss of Control Room Controls, Adequacy of Backup Instrumentation," and is closed as a restart issue.

3.1.5 Steam Generator Overfill Protection Circuits

This issue is discussed in Section 3.1.3, "Emergency Feedwater Initiation and Control System," and is closed as a restart issue.

3.1.6 Main Steam System Response to ICS/NNI System Failures

This issue is discussed in Section 3.1.2.6, "Loss of Control Room Controls and Indications, Adequacy of Backup Instrumentation," and is closed as a restart issue.

3.1.10 Achievement of Safe Shutdown Using Safety-Related Equipment

This issue is discussed in Section 3.1.2.12, "Licensee's Re-review of IE Bulletin 79-27 Concerns," and is closed as a restart issue.

3.3 Plant Maintenance

3.3.1 Maintenance Program Evaluation

3.3.1.12 Maintenance Program Evaluation, Conclusions

The staff has determined through interviews, witnessing onsite activities, and review of documents that program modifications have and will continue to improve the quality and efficiency of maintenance activities. Staff inspectors will verify implementation of the most recent programmatic changes during and following plant restart. The results will be documented in a timely NRC inspection report after startup. This issue is closed as a restart issue.

3.3.2 Valve Preventive Maintenance Program

In Section 3.3.2 of the restart SER issued October 1987, this item remained open as a restart issue until the licensee's preventive maintenance (PM) program for valves was fully implemented and was inspected by the NRC staff. Since that time the licensee's PM program for valves was reviewed as described in procedure MAP-009, "Preventive Maintenance Program." The details of that inspection are found in Inspection Report 50-312/87-30. By sampling selected valves, the inspection verified that all of the valves identified by the licensee as having operational significance had been included in the program. The inspection verified that most of the specific maintenance requirements (tasks) had been developed to define the exact scope of the program. (After the inspection, on December 16, 1987, the inspector confirmed with the licensee's Maintenance Manager that the small remainder of undefined tasks had been specified since the inspection.) In most cases, the maintenance tasks were derived from vendor recommendations for the particular valve or type of valve. In some cases, after review, the licensee decided that modification of the vendor recommendations to allow greater operational flexibility or reflect different service conditions was appropriate. The inspector found the selected task descriptions reviewed to be adequate.

On the basis of this review, the licensee's description of its valve preventive maintenance program appeared adequate. In particular, the preventive maintenance program for valves appeared to adequately describe the specific maintenance tasks required for all valves important to safe operation of the facility. The NRC staff finds that the PM program for valves is acceptable. This item is closed as a restart issue.

3.4 Training and Operator Performance

3.4.1 Adequacy of Operator Training

3.4.1.1 Review of Training Program

In Section 3.4.1.1 of the restart SER issued in October 1987, it was stated that the NRC staff will report on the resolution of this issue in a supplement to the SER.

During the week of October 26 through 30, 1987, the NRC staff conducted a post-accreditation audit of the training program at Rancho Seco. The non-licensed

and licensed operator training programs were the subject of this review. The criteria used by the staff to audit the implementation of these performance-based training programs are contained in NRC's "Training Review Criteria and Procedures" (NUREG-1220, June 1986). These procedures consist of the criteria against which the five elements of performance-based training are evaluated. The five elements that are essential to this type of training are:

(1) systematic analysis of the jobs to be performed

(2) learning objectives that are derived from the analysis and that describe desired performance after training

(3) training design and implementation based on the learning objectives

(4) evaluation of trainee mastery of the objectives during training

(5) evaluation and revision of the training based on the performance of trained personnel in the job setting

The staff selected six tasks for each of the programs from the Rancho Seco task lists. The audit consisted of document review, interviews and interactions with both training and operations staff and management, and classroom observations. These procedures were conducted to respond to the questions posed in NUREG-1120. The post-accreditation review of the five elements of performance-based training at Rancho Seco resulted in the following findings:

- The analysis of jobs (in this instance, the non-licensed and licensed operator positions) was done by adapting the Institute of Nuclear Power Operations (INPO) task data base and modifying it to reflect tasks specific to Rancho Seco.

- The results of this analysis were validated through a survey of job incumbents; tasks were identified for both initial and continuing training.

- Knowledges, skills, and abilities were identified through the development of enabling objectives to support terminal objectives. Standards and conditions for learning objectives were included by exception, with the implied standard of 100% accuracy and a condition of "from memory" for those objectives that do not include specific standards and conditions.

- The design and implementation phase of the program was appropriately implemented and the training department has an ongoing program that continues to make relevant training procedures more comprehensive.

- Lesson plans are of high quality and training is delivered effectively. However, the staff suggested that training for certain operator tasks could be improved by using actual tools or equipment task simulators rather than relying on transparencies which only show the equipment.

- Both trainee and program evaluations are implemented through a number of effective feedback loops that are either proceduralized or included in program descriptions.

- Instructors are evaluated on a regular basis.

- Review of task-related documentation indicates that all instructor, trainee, and program evaluation feedback is routinely used to improve training programs.

The staff finds that the licensed and non-licensed operator training programs at Rancho Seco are adequate to support restart. This issue is closed as a restart issue.

3.4.1.4 Emergency Procedure Training

In Section 3.4.1.4 of the restart SER issued in October 1987, it was stated that before startup the NRC staff will reevaluate the licensee's emergency response training program including emergency response training for the control room staff.

In addition to the specific training conducted discussed previously, and documented in Inspection Reports 50-312/86-06, 86-07, 86-32, and 87-06, a final integrated evaluation of licensed operator training on the final emergency operating procedures was conducted and documented in Inspection Report 87-32 (Paragraph 9). This inspection evaluated the knowledge level of operators with respect to their responsibilities and required actions during emergencies. Four senior reactor operators and four reactor operators were interviewed in the course of this evaluation. The inspectors concluded that the licensed operators were, in general, adequately trained on the final emergency operating procedures, and the emergency procedures training program is acceptable.

Emergency procedures training is closed as a restart issue.

3.4.1.7 Operator Retraining Due to Long-term Shutdown

Section 3.4.1.7 of the restart SER (NUREG-1286) issued in October 1987 contained a discussion of the licensee's program to address the effect of the long-term shutdown period on operator performance. In February 1987, the NRC staff inspected operator retraining necessitated by the long-term shutdown (some 26 months) (see Inspection Report No. 50-312/87-06). At that time, the licensee had not completed training on the final revised procedures. Since that time, the licensee has completed training on the final revised procedures. The licensee completed training on its emergency operating procedures (EOPs) before the NRC staff inspection later documented in Inspection Report No. 50-312/87-32 in October 1987. That inspection (Section 9 of the inspection report) documented that the licensee had implemented a complete and acceptable program of training for EOPs.

In addition, although the licensee's formal training of its operators has been thorough and comprehensive, some period of refamiliarization by the operators can reasonably be expected from the 26-month duration of the outage. The licensee has attempted to compensate for this with an elaborate and slow testing and power ascension program. The adequacy of the operator training will, therefore, continue to be evaluated by Region V personnel throughout the testing and power ascension program with the resident inspection program, the operational readiness inspection before restart, and the extended enhanced operational inspection during power ascension.

The licensee's program of operator retraining necessitated by the long-term shutdown is found to be acceptable, and this issue is closed as a restart issue.

3.5 Plant Normal and Emergency Procedures

3.5.6 Adequacy of Emergency Operating Procedures

Section 3.5.6 of the restart SER (NUREG-1286) issued in October 1987 addressed the adequacy of the licensee's emergency operating procedures (EOPs).

This item had been previously reviewed as part of Inspection Nos. 50-312/86-07, 86-08, and 87-32. During the inspection, it was found that the EOPs had not been developed according to an approved Procedures Generation Package (PGP) as required by Supplement 1 to NUREG-0737. The licensee has since developed an approved PGP which incorporates the required features called for in Generic Letter 82-33, "Requirements for Emergency Response Capability." Specifically, Generic Letter 82-33 requires each licensee to submit to the NRC a PGP which includes:

(1) plant-specific technical guidelines
(2) a writer's guide
(3) a description of programs for validation and verification of EOPs
(4) a description of the training program for the upgraded EOPs

The staff has since evaluated the Rancho Seco PGP, originally submitted by letter dated January 31, 1984, with supplemental submittals dated June 16, November 20, and December 9, 1987. On the basis of the NRC staff review, the PGP for Rancho Seco is found to meet the requirements of Supplement 1 to NUREG-0737 and Generic Letter 82-33, and is acceptable.

A later inspection was completed in December 1987 which addressed the licensee's program for preparation and implementation of the EOPs following extensive changes to portions of the program that were incomplete or undocumented. That inspection, No. 50-312/87-47, concluded that the licensee had adequately implemented the revised PGP dated November 20, 1987 and amended December 9, 1987 into EOPs. It is concluded that the licensee's EOPs are adequate for restart of Rancho Seco, and this issue is closed as a restart issue.

3.7 Systems Review and Test Program

3.7.3 Review of Test Procedures and Systems Testing

Section 3.7.3 of the restart SER (NUREG-1286) issued in October 1987 noted that the licensee's test procedures and systems testing programs would continue to be inspected by the NRC staff. The licensee had not then completed a sufficient number of tests for an evaluation to be made. Since then, the NRC staff has inspected and reviewed the licensee's test procedures and system testing. From these further inspections it is concluded that the licensee's test program requirements outlined in the system status reports of the system review and test program have been adequately implemented by required test procedures, analysis, or a combination of these. Satisfactory completion of this test program by the licensee should ensure that all of the systems selected for

testing, which comprise all of those important to plant operation and safety, are adequate for restart of Rancho Seco.

The actual conduct of system testing is observed continuously by the assigned resident inspection staff. The reports of these observations are available, but are not appropriate for inclusion in the SER and its supplements. The overall conclusion from these reports is that the licensee's performance of the testing has been satisfactory to date.

On the basis of NRC staff inspections performed to date, and conclusions drawn from these inspections, the licensee's test procedures and systems testing programs are acceptable. This issue is closed as a restart issue.

3.8 Licensee Management and Organizational Considerations

In Section 3.8 of the restart SER issued October 1987, it was stated that the staff will inspect the full implementation of the revised organization before restart and will address the results of that inspection in a supplement to the SER or in an NRC inspection report.

The staff has addressed the new organizational structure under the Chief Executive Officer (CEO), Nuclear, and found the organizational structure to be acceptable. The staff's SER also discussed the qualifications of key managers in the Rancho Seco organization. The staff concluded that individuals selected for the positions of CEO, Nuclear; Assistant General Managers (AGMs) for Nuclear Power Production and Technical and Administrative Services; and the Directors responsible for Nuclear Operations and Maintenance, as well as for Technical Services and Plant Support, have backgrounds and experience suited to these positions.

The Region V staff has continued to examine the licensees's efforts to fill permanent positions in the revised organization. The organization under the CEO, Nuclear has an authorized staffing level for the year ending December 1988 of 1056 positions. The licensee has filled more than 80% (approximately 865) of these positions are with permanent personnel. Essentially all remaining authorized positions are currently filled by acting licensee or contract personnel, and goals have been established for filling all positions with permanent licensee personnel by the end of 1988. The majority of unfilled positions are at the engineer and technician level in the areas of nuclear engineering (25); nuclear plant support - chemistry, health physics, and entry level maintenance and non-licensed operations personnel (74); administrative support personnel - information systems analysts and clerical personnel (50); and quality assurance - associate quality engineers and inspection personnel (12).

The Region V staff has also reviewed the qualifications of key managers at the department level, and finds that the licensee has, with a few exceptions, filled these positions with experienced permanent personnel.

(1) The Manager Maintenance Department position is currently filled with a contractor. This individual has approximately 10 years of U.S. Navy nuclear experience and 8 years of commercial nuclear power plant experience, including the positions of Senior Field Service Engineer with Babcock and Wilcox in the development and implementation of preventive maintenance

and equipment trending programs and Nuclear Maintenance Superintendent at the Crystal River Nuclear Plant. This person served as a consultant for surveillance testing and maintenance management at the San Onofre Nuclear Generating Station during startup of Units 2 and 3. The licensee expects to fill this position by the end of March 1988.

(2) The position of Manager Plant Performance Department is currently filled by an experienced individual on loan from INPO. This individual has held various management positions at INPO during the past approximately 5 years in the Operations Department and the Maintenance and Events Analysis Department; he also has approximately 4 years of U.S. Navy nuclear experience and approximately 10 years of commercial nuclear power plant experience. He has held positions of maintenance and operations superintendent at the Big Rock Point Nuclear Plant. This individual is to remain on loan from INPO through September 1988; during this time, the licensee plans to complete the selection of a permanent replacement for this position.

(3) The Manager Operations Department has approximately 15 years of commercial nuclear power plant experience, and has held positions progressing from Assistant Nuclear Operator through Shift Supervisor as well as Shift Technical Advisor and Training Manager at the Crystal River plant. He held a Senior Reactor Operator License at Crystal River Unit 3, and obtained a Bachelor of Science degree in electrical engineering in 1985. He has held his current position at the Rancho Seco plant since February 1987.

(4) The Manager Nuclear Engineering Department is a graduate of the U.S. Naval Academy and served in the navy nuclear program for approximately 5 years; during this time, he was qualified as an Engineering Officer of the Watch. He has approximately 7 years of experience with the Bechtel Power Corporation, where he held positions of Project Engineer responsible for containment integrated leak rate testing for all Bechtel Offices, as well as Project Engineer supervising a multi-discipline engineering staff responsible for completing the design and startup support for Diablo Canyon Unit 2. He also held the position of Chief Mechanical/Nuclear Engineer at the Bechtel Office in San Francisco before being selected for his current position at SMUD in September 1986.

(5) The Director Nuclear Quality and Managers of the Nuclear Licensing, Environment Protection, Material Control, Radiation Protection, Chemistry, Training, and Modifications Departments all have backgrounds and experience suited to these positions. Their related commercial nuclear plant experience ranges from 12 to 17 years per person. With the exception of the Manager Modifications Department, all hold bachelors' degrees or higher with studies in the fields of engineering or a related science.

(6) The Director Nuclear Quality and all department level managers have been determined by the Region V staff to have acceptable backgrounds and experience and meet the relevant criteria of applicable sections of NUREG-0800, the Standard Review Plan.

On December 23, 1987, the Administrator of Region V issued a letter to the licensee under the provisions of 10 CFR 50.54(f) regarding management and personnel

considerations associated with the control and reporting of liquid effluents from the Rancho Seco plant during 1985. The letter requires the licensee's senior management to provide in writing within 30 days its assessment of its faith and confidence in the present management personnel who were, or may have been, involved in the control and reporting of liquid effluents from the Rancho Seco plant during 1985.

The staff is evaluating the licensee's response to this 10 CFR 50.54 action in determining the extent of enforcement action to be taken with regard to the staff's inspection and investigation findings - particularly with respect to management involvement in the control and reporting of radioactive effluents.

The issue of licensee management and organization considerations is closed as a restart issue.

4 RESOLUTION OF CONCERNS NOT RELATED TO THE DECEMBER 26, 1985 EVENT

4.1 Postaccident Sampling System

4.1.3 PASS Procedures and Training

Section 4.1.3 of the restart SER (NUREG-1286) issued in October 1987 stated that although postaccident sampling system (PASS) procedures and training had been inspected, a number of items were still open, and the staff would inspect the licensee's PASS training and procedures further to verify they are ready for startup.

The licensee has since completed revising the PASS operating procedures. A training program consisting of both classroom and on-the-job training has been implemented. A retraining program has been established and training is being provided to support personnel peripherally involved with the PASS.

By reviewing the records and by direct observation, the NRC staff verified that the licensee has fully trained and qualified five technicians to operate the postaccident sampling system. The inspection findings are documented in NRC Inspection Report No. 50-312/88-01. These findings provide a reasonable basis to conclude that the PASS can be operated consistent with the position stated in NUREG-0737, Item II.B.3, and is acceptable. This issue is closed as a restart issue.

4.1.4 PASS Testing

Section 4.1.4 of the restart SER (NUREG-1286) issued in October 1987 stated that testing of all aspects of the operation of the PASS cannot be completed until the plant is in a hot shutdown condition, at full pressure and temperature. The licensee had stated that all essential operating parameters would be fully tested before restart to demonstrate that the system will operate reliably and will produce accurate analytical results that comply with its commitments to the requirements of NUREG-0737.

The NRC staff inspected the PASS and documented the results in Inspection Report Nos. 50-312/86-37, 50-312/87-05, and 50-312/87-22 (see item 86-37-01). At the time of these inspections, a number of issues were open.

The licensee has since completed functional testing of the PASS. The testing was conducted in accordance with written procedures that contained clearly identified objectives designed to verify the performance of the system. Simulations appropriate for the cold shutdown condition of the reactor were performed using a pressurized sample source. These tests confirmed the system's ability to reduce pressure, cool the sample, and make the required analyses.

The licensee plans to perform an integrated demonstration of the PASS capability when the reactor is operating at about 15% power.

The NRC staff reviewed the licensee's testing program and observed several of the tests being performed. The inspection findings are documented in NRC Inspection Report No. 50-312/88-01. These findings provide a reasonable basis to expect that the PASS will be able to perform its design functions, and is acceptable. This issue is closed as a restart issue.

4.2 Control Room/Technical Support Center Heating, Ventilation, and Air Conditioning System

4.2.2 HVAC Testing

Section 4.2 of the restart SER (NUREG-1286) issued in October 1987 identified two issues that need to be resolved before startup. These are:

(1) The licensee's review and validation of its system design habitability report will be reviewed by the staff.

(2) The staff will inspect the modified control room/technical support center (CR/TSC) HVAC system before restart to verify operability.

After the December 26, 1985 event, the licensee significantly modified the CR/TSC HVAC system in order to improve its capability and performance. In order to address the above issues, the staff reviewed information on the system design modifications against the criteria of Standard Review Plan (SRP) Sections 6.4 and 9.4.1 to confirm that the system can perform its habitability safety functions in the event of a radiological or toxic gas emergency. From this review, the staff finds that the modified CR/TSC HVAC system meets the applicable criteria as discussed further below.

The staff reviewed the licensee's "CR/TSC Habitability Report," Revision 5, submitted by letter dated July 22, 1987 and additional information requested by the staff submitted in letters dated January 13, February 10, and February 25, 1988. The staff also inspected the modified CR/TSC system (November 10-12, 1987 and February 4-5, 1988) to verify its operability and reviewed numerous licensee documents (procedures, test results, engineering change notices, calculations, drawings, system status reports, vendor data, training programs, and licensee event reports) in conjunction with the inspection.

As part of the CR/TSC HVAC system inspections, the staff observed the licensee perform surveillance procedure SP 84A(B), "Monthly Surveillance Test of CR/TSC Essential Ventilation System Loop A (Loop B)." This procedure demonstrates the operability of the redundant CR/TSC essential ventilation system trains every 31 days in accordance with Technical Specifications (TS) 4.10.1.A and 4.10.1.D. Among the acceptance criteria for this procedure are the following:

(1) Air flow through the high-efficiency particulate air (HEPA) and charcoal filters in the essential filter unit was initiated (TS 4.10.1.A).

(2) The CR/TSC essential filtering system started on a manual signal and operated for at least 15 minutes (TS 4.10.1.D).

(3) All system dampers cycle to the indicated positions for normal, radiation, and toxic gas modes.

(4) Pressure in the CR/TSC is maintained at least 0.25 inch above outside atmospheric pressure by operation of the CR/TSC essential system in the radiological mode.

The staff identified no concerns in connection with the observed performance of the procedures and finds, based on the performance of this and other procedures, that system operability has been satisfactorily demonstrated.

The licensee also performed maintenance procedure M-111, "HVAC Maintenance Procedure for Air Balance of Ventilation Systems," for the CR/TSC essential ventilation system, loops A and B. In this procedure, duct velocity probe traverses were made to determine pertinent air flow rates in each operating loop for the radiation and toxic gas modes of operation. Traverses in the idle loop were also made. The data, results, and an explanation of the results were provided to the staff for review. The staff indentified no issues in connection with its evaluation of the information provided and finds that proper air flow have been demonstrated.

The staff determined that the performance and results of these and other test procedures were consistent with the rates of air inleakage to the CR/TSC assumed in the staff's radiation dose calculations and in the toxic gas analyses. The results do not indicate the presence of a system malfunction or condition of inadequate CR/TSC boundary integrity that would invalidate the assumed rates of air inleakage. The staff finds that control room leak tightness has been acceptably verified.

Considering this review of the operability and performance of the CR/TSC HVAC system before restart, the staff concludes that adequate system functional performance has been demonstrated and the criteria of SRP Sections 6.4 and 9.4.1 for ensuring postaccident control room habitability have been satisfied except for the four items noted below. It should be noted, however, that the licensee has made acceptable commitments for restart concerning the four long-term items as follows:

(1) Chlorine will not be permitted on site except in amounts of less than 100 pounds for use in sewage treatment until the issue concerning the location of chlorine detectors has been resolved with the staff.

(2) The licensee is conducting tests and will submit an 18-month report of results to the staff regarding the long-term adequacy of the silicone sealants employed to maintain the control room envelope integrity.

(3) The licensee will by June 1, 1988 make the necessary changes, acceptable to the NRC staff, to resolve the potential problem of personnel incapacity in the CR/TSC from ammonia gas drawn in through the HVAC intake following an ammonia tank rupture.

(4) The licensee will take the necessary measures before startup after the first refuel outage following restart to resolve the potential problem of excessive radiological dose to control room personnel following an accident. Meanwhile, the licensee will employ proposed and acceptable mitigative measures for control room personnel protection.

On the basis of the foregoing considerations, including acceptable commitments by the licensee as noted above, the issue of the CR/TSC HVAC system is closed as a restart issue.

4.3 Radioactive Liquid Effluent Releases

The licensee has implemented a comprehensive program to improve control of radioactive liquid effluents. The program is described in the attachment to the licensee's letter GCA 88-068 dated February 3, 1988 and in the "Radiological Effluent Control Manual," RECM-6878, Revision 0, dated February 1988. These program documents address the administrative aspects of effluent control and identify the major components. The major components are discussed separately in the paragraphs that follow.

4.3.1 Technical Specifications

The existing Technical Specifications require that liquid effluents be controlled; "control" includes meeting the dose design objectives of Appendix I to 10 CFR Part 50. Some changes were necessitated by equipment changes and other changes were indicated by past problems. To meet these needs and make other improvements, the licensee proposed a major revision of the effluent control parts of the Technical Specifications. These changes (Proposed Amendment 155, Revision 2) are delineated in the enclosure to Sacramento Municipal Utility District, SMUD (licensee) letters AGM/MPP 87-476, December 23, 1987 and AGM/NPP 88-100, February 11, 1988.

The proposed changes in the lower limits of detection (LLD) for liquid effluents are important for coping with the special problems posed by the dry site at Rancho Seco. Specifically, the LLD for Cs-134, Cs-137, and for other principal gamma emitters are being reduced by a factor of 199, to 4 pCi/L. This ensures that releases would be detected if they were capable of producing doses that would be a small fraction of the Appendix I dose criteria. Thus, these LLD values are acceptable.

The staff has reviewed the proposed changes to the Technical Specifications and concludes that, as indicated by the licensee, four categories of changes exist: (1) clarifications of existing requirements, (2) revisions to achieve greater consistency with the Standard Technical Specifications, (3) corrections required by modifications of the equipment, or (4) requirements made more stringent to accommodate the special conditions at Rancho Seco. It is concluded further that the proposed changes are consistent with the intent of the Standard Technical Specifications and are acceptable.

4.3.2 Radioactive Liquid Effluent Treatment System Modifications

The licensee has made significant changes in the liquid effluent treatment systems to improve Rancho Seco's capability for operating within the dose criteria of Appendix I to 10 CFR Part 50. These changes are described in the following SMUD letters and the enclosures thereto: (1) JEW 87-586, dated April 15, 1987; (2) GCA 87-763, dated November 12, 1987, and (3) GCA 87-916, dated January 7, 1988. Also an evaluation of the modified system's ability to adequately control and process liquid effluents is presented in the enclosure to GCA 87-810, dated January 13, 1988.

The major elements of the modifications are (1) increasing dilution water flow to 8500 gpm, (2) installation a new retention tank (RHUT-C) and the associated piping to keep uncontaminated water separate from contaminated water, (3) adding a demineralizer system to remove radioactivity from the contaminated secondary water, (4) installing control measures so the contaminated water (from RHUT-A and RHUT-B) cannot be directly discharged to the environment, and (5) obtaining more sensitive instrumentation for analyzing liquid samples. Further, the use of disposable resins in the condensate polishing demineralizers (which had been initiated earlier) was made a permanent part of the system.

The effectiveness of the modification will depend on how the new demineralizers are operated. The demineralizers are most effective when operated in a once-through mode; to achieve a high level of decontamination in the recirculation mode, the water must pass through the demineralizers repeatedly (i.e., approximately 5 times for decontamination by a factor of 100). The recirculation mode appears necessary, however, to permit the waste water to be treated chemically before demineralization, so the resins are not poisoned. Thus, the demineralizers can be highly effective, but only if the volume of liquid waste is kept small compared with the demineralizer capacity. In the evaluation, credit for the demineralizers was conservatively limited to a factor of 2. With this credit, the system is capable of coping with releases at the levels being experienced before shutdown on December 26, 1985. The system could not accommodate higher releases, such as those experienced in 1983 and in 1984, unless the demineralizers were highly effective.

The licensee is not relying on the system modifications alone to hold releases to the Appendix I levels; a comprehensive program exists for liquid effluent control. This program ranges from limiting the levels of radiocesium in the primary system to minimizing leakage from the secondary systems. The staff has reviewed this program and concludes that the program and the systems modifications combined are sufficient to permit operation of Rancho Seco within the relevant criteria.

The staff also reviewed the design for modifying the liquid effluent system. The systems were designed in accordance with the provisions of Regulatory Guide 1.26 and 1.143. Appropriate provisions have been made for spill control and for the control of external radiation. The system modification design meets the acceptance criteria of Section 11.2 of the Standard Review Plan (NUREG-0800) and is acceptable.

4.3.3 Offsite Dose Calculation Manual

The Offsite Dose Calculation Manual (ODCM) for Rancho Seco was revised to reflect the changes in the effluent control systems and to incorporate certain other improvements. Revision 5 to the ODCM was submitted with SMUD letter GCA 87-908, dated December 27, 1987. The staff has reviewed this document. Minor typographical errors in Tables A-3 and A-4 were called to the attention of the licensee. These should be corrected in the next revision of the ODCM, though they are not important enough to affect the acceptability of the document. The staff has concluded that Revision 5 of the Rancho Seco ODCM was prepared in accordance with the guidance provided in NUREG-0133 and Regulatory Guide 1.109, Revision 1, and is acceptable.

4.3.4 Radiological Environmental Monitoring Program Manual

The Radiological Environmental Monitoring Program (REMP) Manual is a document unique to Rancho Seco. It contains information about the radiological environmental monitoring program that commonly is included in the ODCM. The REMP Manual was updated to reflect the change in Technical Specification 1.22 of proposed Amendment 155. Revision 1 to the REMP Manual was submitted with SMUD letter AGM/TA 87-211, dated November 11, 1987. The staff has reviewed this document and concludes that it is consistent with the proposed Technical Specification 1.22 and with the guidance provided with the NRC letter from W. P. Gammill to all power reactor licensees, dated November 27, 1979. Therefore, Revision 1 to the REMP Manual is acceptable.

4.3.5 Radioactive Liquid Effluent Releases, Conclusions

The NRC staff has evaluated the licensee's proposed Technical Specifications for radioactive liquid effluent releases, the effluent system modifications, the Offsite Dose Calculation Manual, and the Radiological Environmental Monitoring Program (REMP) Manual. The proposed Technical Specifications, system modifications, and the ODCM and REMP Manual are acceptable for plant restart. This issue is closed as a restart issue.

4.4 Emergency Plan

4.4.2 Emergency Plan Training

Section 4.4.2 of the restart SER (NUREG-1286) issued in October 1987 noted that the NRC staff's Inspection Report No. 50-312/86-14 had identified numerous violations in the licensee's emergency response training program. The licensee's corrective action for those violations consisted of numerous initial and long-term actions. NRC Inspection Report No. 50-312/87-02, reporting on an inspection conducted in March 1987, evaluated the licensee's initial corrective actions and determined them to be adequate. Because that report also identified numerous areas that still required improvement, the staff would need to reinspect the emergency response training program. The status of the long-term corrective actions and the improvement items would also need to be inspected before restart.

NRC staff reinspected the Emergency Preparedness Training Program in October and November 1987 and January 1988. The staff confirmed that the licensee had adequately addressed all areas requiring improvement before restart. The details of these items and the inspection of them are in Inspection Report Nos. 50-312/87-33 (Section 5) and 50-312/87-46 (Section 2). These findings provide a reasonable basis to conclude that the licensee's emergency plan training is acceptable for restart. This issue is closed as a restart issue.

4.4.3 Emergency Plan Implementation Procedure and Dose Assessment

Section 4.4.3 of the restart SER (NUREG-1286) issued in October 1987 noted that the licensee was revising the emergency plan and the emergency plan implementing procedures (EPIPs). Procedures for dose assessment, training, classifications, and drills and exercises were also being revised. The NRC staff would then need to inspect these areas again before restart and would discuss the results of its inspection in a supplement to the restart SER or in an NRC inspection report.

The staff has since that time reinspected the licensee's emergency plan, emergency plan implementing procedures, and procedures for dose assessment, training, classifications, and drills and exercises. The staff confirmed that the licensee has adequately addressed all areas requiring improvement. The details of these items and the review of them are in Inspection Report Nos. 50-312/87-33 (Section 3) and 50-312/87-46 (Sections 2 and 4). In addition, the acceptability, with additional minor changes, of the emergency plan was the subject of separate correspondence (January 12, 1988, letter from R. Fish, NRC, to G. C. Andognini, SMUD). These findings provide a reasonable basis to conclude that the licensee's emergency plan implementing procedures and dose assessment procedures are acceptable for restart. This issue is closed as a restart issue.

4.6 Safety Parameter Display System

The safety review of the upgraded safety parameter display system (SPDS) given in the Rancho Seco restart SER (NUREG-1286) was incomplete in the following technical areas:

(1) equipment qualification
(2) fire protection
(3) common mode faults
(4) qualification of isolation devices
(5) software validation

Between October 26 and 28, 1987, the staff, with the assistance of consultants, conducted an onsite audit of the licensee's upgraded SPDS. The consultants reported to the staff in the Site Audit Report. The results from the audit and the review of subsequent submittals from the licensee serve as the basis for the safety evaluation that follows.

4.6.2 SPDS Design Issues and Evaluation

Equipment Qualification and Reliability

The staff requested that the licensee provide documents and data that demonstrate that the upgraded SPDS complies with industry standards and regulatory criteria for safety-related systems. The licensee's response (letter dated November 20, 1986) contained commitments and described work performed to qualify equipment. The licensee stated that only sensor inputs need meet environmental qualification since all portions of the system except field sensors operate in a mild environment. Equipment located outside the reactor building will be designed for use in the area of service. The design goal for this equipment is a 40-year service life and a design-basis accident (DBA) radiation dose.

The upgraded SPDS will be a quality assurance (QA) Class 1 and seismic Category I system. Circuits having direct interface with SPDS cabinets will be Class 1 and routed in Class 1 raceways. Also, the electrical power will be from Class 1 uninterruptible power supply (UPS) systems.

During its onsite audit of October 26-28, 1987, the staff evaluated equipment qualification using written criteria and guidelines for the evaluation. The significant documentation on equipment qualification was reviewed during the audit.

The reviewers encountered difficulties in evaluating test data. Initial findings were:

(1) With the exception of data on the SPDS computer, the documentation does not include postseismic electrical performance data on the upgraded SPDS.

(2) With the exception of the bus isolators, the electrical isolation devices may not be qualified to all of the requirements imposed on the upgraded SPDS.

(3) It could not be determined if the central control unit (CCU) components failed because of the lack of a brace or if they would have failed even had the brace been present.

(4) The central switching unit (CSU) could be a single point failure (it contains both channels A and B) under seismic conditions. No documentation showing that the CSU successfully passed seismic and functional testing was provided.

During the audit, the staff requested that the licensee develop a matrix matching display system components to the requirements of IEEE Standard 323-1974. The staff requested that the licensee certify the qualification of equipment for each element of the matrix and provide justification for use of the component if it does not meet a requirement.

Also during the audit, the staff conducted a hardware walkthrough of the display system, from multiplexers to display devices. The walkthrough identified problems in the following cabinets:

H4CDAL

(1) The open card cages of the CCUs should be covered in a manner acceptable to the NRC staff.

(2) The rear of the CSU should be permanently attached to the lower support bracket, or documentation should be provided showing that the attachment is not necessary for seismic conditions.

H2SP

The cathode-ray tube (CRT) circuitry and glass should be protected. The licensee and the manufacturer should provide a method by which the CRT can be protected. The method must be acceptable to the NRC staff. An inspection will be performed to ensure acceptability of the protective measure taken.

All Cabinets

(1) Cables that pass over metal edges must be protected.

(2) Cables must be supported in such a way that they cannot whip during a seismic event.

(3) Friction fit connectors must be secured in such a way that they cannot work loose.

(4) Items that are not a part of the SPDS system must be removed from the cabinet.

(5) Spare conductors must be properly terminated.

The staff's major concerns are with the problems identified in cabinets H4CDAL and H2SP. A single failure could potentially result in the total loss of display capability. The contractor's Site Audit Report provided additional details on these concerns. During the audit's exit briefing, the staff discussed these concerns with the licensee and requested that the licensee resolve these issues.

By letters dated November 9, November 20, and December 23, 1987, the licensee responded to staff concerns. The staff also used data from the Site Audit Report in its review. The November 20, 1987 letter contains a matrix that identifies display system components in terms of equipment qualification. The staff review of this matrix focused on the seismic qualification of system components. The results from that review follow.

Data in the Site Audit Report indicate that the display monitors meet seismic requirements. A display pattern served as a pre- and post-test measure of performance. Staff review of the seismic test report during the onsite audit indicated that the post-seismic test display pattern matches the pre-test pattern. The staff finds this acceptable for meeting the seismic requirement.

In the December 23, 1987 letter, the licensee described the seismic qualification of the uniplex field multiplexer, central control unit, central switching unit, and isolators. National Testing Systems qualified these components seismically. The equipment tested was similar to the equipment installed at Rancho Seco. The components tested in the uniplex field multiplexer included power supplies, input terminal blocks, bus isolators, ac circuit breakers, and receptacle ac outlet boxes. Functional tests of the multiplexer before and after the seismic test were successful. The staff finds these results acceptable for the multiplexer, circuit breakers, and power distribution boxes.

In the original seismic test of the central control unit and the central switching unit (letter dated December 23, 1987), only one of the two central control units passed and functioned after the test. Subsequently, a reanalysis of the entire Rancho Seco seismic requirements resulted in less severe seismic qualification curves for this equipment. The licensee contracted with National Testing Systems and Action Environmental Testing Corporation to analyze tests performed by Wyle Laboratories on a similar unit that contained central control units and a central switching unit. Also, the licensee added braces within the cabinet to support the central switching unit. The licensee's contractor found that the spectra in the successful Wyle test of similar equipment enveloped the revised Rancho Seco spectra. The margin of the envelope was not evaluated. Furthermore, the licensee hired another contractor to perform a third-party review of these results. The third-party review affirmed the previous analysis. Based on the revised spectra, it is the staff's engineering judgment that the above equipment is seismically acceptable.

In the seismic tests described above for the central control unit, central switching unit, and uniplex field multiplexer, the circuit boards within these devices contained isolation devices. The isolation devices are an integral

part of the printed circuit board. Also, the isolation devices are small electronic devices (i.e., integrated circuit optical isolators, pulse transformers, and isolation transformers) that have no moving parts and should not change state because of a seismic event. Based on these considerations, it is the staff's engineering judgment that the isolators are seismically acceptable.

The staff also reviewed equipment qualification (letter dated November 20, 1987) for susceptibility to radiofrequency interference, electromagnetic interference, temperature, humidity, radiation, and traceability of components. The staff's review of the licensee's matrix (letter dated November 20, 1987) concludes that the display system components meet many of the requirements. The licensee provides justification (letter dated November 20, 1987) when a component does not fully meet a requirement. The staff's review of the justifications finds them to be reasonable. The staff also found that the licensee proposes to increase technical specification surveillance to ensure SPDS operability.

The staff requested that the licensee provide quarterly performance reports (beginning with restart) on the operation of the display system. In the November 9, 1987 letter, the licensee agreed to provide the reports. Also, the staff requested that the licensee compare the reliability between the digital data/display channel (upgraded SPDS) and an analog data display. In the November 20, 1987 letter, the licensee agreed to provide the comparison after restart; this committment is acceptable to the staff.

In the November 20, 1987 letter, the licensee described several improvements to the display system. These improvements consist of:

(1) a barrier to separate the central control units

(2) a retainer bar to hold circuit boards in place for each central control unit

(3) the central switching unit secured to the support brace

(4) a cover for the electronic components and tube for each cathode-ray tube

(5) metal edges protected to prevent cable damage

(6) a commitment to clean up the cabinets to resolve staff concerns on whip of unsupported cable during a seismic event

(7) a commitment to review friction connectors, and if deemed necessary, installing new devices to ensure the connection

The staff reviewed these improvements and commitments and finds them acceptable. The staff will perform a timely confirmatory inspection.

In accepting the limitations of the equipment qualification discussed above, the staff considered the type of display in this system. The basic metaphor for the SPDS interface is a model of the process. The model consists of a pressure-temperature plot of water (presented as graphic segments on a cathode-ray tube). It contains the saturation line between liquid phase water and vapor phase steam. The model also contains the current values of primary coolant pressure, hot-leg temperature, and cold-leg temperature. The saturation

temperature of secondary coolant water is also presented. From the structure of the data within the model, a user easily evaluates the cooling of the reactor core and the status of the heat transfer from the primary coolant to the secondary coolant. These data are most useful during post-trip operation of the plant.

The format of the model-based display (described above) should be very useful to the control room operators. The data structure within the model directly supports the evaluation of a critical safety function, the cooling of the core. Furthermore, the operator may quickly evaluate the phase of the coolant water (subcooled liquid, saturated liquid and vapor, superheated steam) from the displayed data. This eliminates the need for the operator to gather data from individual instruments in various control boards, evaluate the data, and then determine the status of the core cooling and heat transfer from the primary coolant system. These attributes of the display should minimize human error in the use of the system.

Fire Protection

The licensee described the display system's compliance to the requirements of Appendix R in the letter dated November 9, 1987. Circuits of those variables required for Appendix R events are routed through the fire areas for that particular channel. Circuits for channel A variables pass through channel A fire area and circuits for channel B variables pass through channel B fire areas. In fire areas where circuits of channel A and channel B coexist, circuits of the channel not belonging to that fire area have been wrapped, except inside the control room.

During the staff's onsite audit of October 26-28, 1987, the audit team visually inspected fire-wrapped cables. In the first location, the routes for channel B cabling from the SPDS control panel to the SPDS computer were outside the confines of the control room through the channel A fire area. The wrap for this section of channel B cabling was one-hour fire wrap consisting of three layers of 3M fire wrap tape (part No. E54A). Also during the onsite audit, the staff noted that the metal supports for the cable trays were wrapped with fire wrap tape. The staff did not evaluate the quality assurance and quality control (QA/QC) documentation associated with the fire wrapping of these cables.

In the November 9, 1987 letter, the licensee stated that the remaining locations for fire wrap are between multiplexers where data bus cables are redundant and identical and where the same cables are entirely outside the confines of the control room. One data bus cable between multiplexer 7 and multiplexer 1, and one data bus cable between multiplexer 9 and multiplexer 1 have been supplied with three-hour fire wrap consisting of three layers of 3M fire wrap tape (part No. E50D).

Based on the above data, the staff finds the fire wrapping of the cables associated with the upgraded SPDS acceptable.

Common Mode Faults

The staff requested that the licensee describe the features of the design process and of the display system that serve as guards against common mode failures/errors. The licensee responded to the request in a letter dated November 20, 1986.

The licensee's display system is a two-channel system. Independent Class 1 battery/diesel-backed ac power supplies provide electrical energy to each channel of the system. Each processor within a channel polls all of the sensors in channel A and channel B through a data bus. Isolation devices serve to separate the instrument channels from one another.

The central switching unit controls the sensor polling operation from the processor within each channel. The central switching unit communicates with each channel through isolation devices. As all sensors within channels A and B are polled, the central switching unit coordinates the polling process. This ensures that each channel's processor is not polling a sensor at the same time. The licensee states that the single failure of the central switching unit results in the loss of one channel in the display system. The redundant channel continues to provide all of the data polled from the sensors.

During its onsite audit, the staff witnessed single-failure testing of the display system. The test results indicated that the display system was not prone to failure when subjected to a single electrical or mechanical failure. The central switching unit always sensed that a central control unit had become inoperable and switched to the non-faulted central control unit. In a demonstration of a failure of the central switching unit, one channel of the display system remained operable.

Also during its onsite audit, the staff performed a walkdown of the display system. The staff noted that the central control units were open card cages, stacked one above the other. The staff expressed a concern that a failure in the top card cage may result in falling debris, which could cause the lower card cage to fail. This would result in the total loss of the display system. The staff asked the licensee to address this concern.

By letter dated November 20, 1987, the licensee described a barrier for separating the open card cages. The licensee stated that the barrier will be designed, fabricated, and installed before restart. In addition, retainer bars to hold the circuit boards in place will be installed before restart. These actions resolve the staff's principal concerns identified in the Site Audit Report. A timely confirmatory inspection of the modified display system will be performed.

The staff's review of the hardware configuration concludes that the independent channels provide adequate protection against common mode faults. Although only one control switching unit exists for the system, the staff judges that one control switching unit is acceptable because it has been demonstrated that failure of the unit does not result in the loss of displayed data in the operating channel.

Qualification of Isolation Devices

The qualification of the isolation devices within the display system was a major issue in the staff's review of the upgraded safety parameter display system. The staff was concerned about the qualification of the devices when subjected to maximum credible fault tests. The licensee had submitted preliminary test results on isolation devices for staff review (letter dated January 12, 1987). Also, in a letter dated April 14, 1987, the licensee described the SPDS isolation methodology it used.

During its onsite audit, the staff completed its review of the final test reports for the isolation devices. Also, in the letter dated November 20, 1987, the licensee stated that its review of the final test reports found no changes with respect to preliminary test results submitted to the staff. Staff review found the devices acceptable for the maximum credible fault tests conducted. Additional details may be found in the consultant's Site Audit Report.

Software Validation

During its onsite audit, the staff evaluated the products of software verification and validation performed by the vendor and the preliminary products of installation tests performed by the licensee. A consultant from Idaho National Engineering Laboratory (INEL) assisted the staff in these efforts. A proprietary vendor (Anatec) document "Safety Parameter Display System, Operating Manual for Sacramento Municipal Utility District, Rancho Seco," describes the computer program in the upgraded SPDS. The "Final Software Verification Report for SMUD SPDS" contains the results from the vendor's software verification and validation efforts.

On review of the vendor's verification and validation products, the staff concluded that all modules were verified and validated to the same level of effort and consistency. Staff review of the documentation concluded it was adequate. The staff also noted that automated tools were used in the verification effort; this should help ensure thorough revalidation after future modifications.

At the time of the staff audit, approximately 70% of the licensee's installation tests were complete. These were independent tests of all signal values and displayed data verified and validated by the vendor. Staff review of the preliminary results from the installation tests noted two discrepancies that should have been discovered by the vendor during validation testing. The staff asked the licensee to address these discrepancies. In the November 20, 1987 letter, the licensee provided additional data for the installation tests. On review of the data and the vendor's test report, the staff concluded that the discrepancies obs rved represented isolated oversights and that there is no fundamental error in the vendor's verification and validation process.

Based on its review of the vendor's test results and the licensee's partial results from installation testing, the staff concludes that an adequate verification and validation program served the development of the software. However, this conclusion is subject to a successful confirmatory review of the licensee's installation test report, which should contain a description of deviations that occurred during testing. In the letter dated November 9, 1987, the licensee committed to provide the staff with this test report as soon as it is available. The staff finds this acceptable and does not consider this confirmatory review a restart issue.

4.6.5 SPDS Review Conclusions

The staff conducted a safety evaluation of the licensee's upgraded safety parameter display system. The initial results from the evaluation are given in a staff memorandum dated July 7, 1987 (F. D. Coffman to G. W. Knighton). The final results from the evaluation, which address equipment qualification, fire protection, common mode faults, qualification of isolation devices, and software validation, are given in the paragraphs that follow.

Equipment Qualification and Reliability

The staff's review of the qualifications of the components of the upgraded safety parameter display system found most requirements were met and the justification for exceptions are reasonable.

To monitor the performance of the system, the staff requested and the licensee agreed to provide quarterly performance reports upon restart of the plant. Also, the staff requested that the licensee compare the reliability between the digital data/display channel (upgraded safety parameter display system) and an analog data display system. The licensee agreed to provide the comparison after restart of the plant, which is acceptable to the staff. Equipment qualification and reliability are acceptable, and this item is closed as a restart issue.

Fire Protection

Based on the observations and data collected during the staff's October 26-28, 1987 onsite audit, the staff finds the fire wrapping of the cables associated with the upgraded safety parameter display system acceptable. Fire protection for the SPDS is acceptable, and this item is closed as a restart issue.

Common Mode Faults

The staff's review of the hardware configurations concludes that the system of independent channels provides adequate protection against common mode faults. The staff review notes that one central switching unit exists for the system. It is the engineering judgment that one control switching unit is acceptable because demonstrated failure of the unit does not result in the loss of displayed data in the operating channel. Common made faults in the SPDS is closed as a restart issue.

Qualification of Isolation Devices

Based on its review of the test results, the staff finds the isolation devices in the display system for the maximum credible faults within the service environment to be acceptable. This item is closed as a restart issue.

Software Validation

Based on its review of the vendor's test results and the licensee's partial results from installation testing, the staff concludes an adequate verification and validation program served the development of the software. The licensee's installation test report, which should also contain a description of deviations identified during testing, will be subject to confirmatory inspection. This item is closed as a restart issue.

Summary

The staff finds the upgraded safety parameter display system acceptable. The items or issues identified above will be confirmed by inspection. The upgraded SPDS is closed as a restart issue.

4.7 Transamerica Delaval, Inc. Diesel Generators

The Rancho Seco Nuclear Generating Station was licensed with an electrical systems design of sufficient capacity to service design safety loads, and with a configuration of two redundant safety trains. The design provided one 4160-V ac emergency diesel generator (EDG) and two 125-V dc batteries in each train of the onsite power system in compliance with General Design Criterion (GDC) 17 of Appendix A to 10 CFR Part 50.

The modification in the plant safety systems design required by NUREG-0737, "Clarification of TMI Action Plan," and NUREG-0696, "Functional Criteria for Emergency Response Facilities," resulted in addition of both ac and dc loads. The existing EDG and battery capacity on each redundant train was found inadequate to supply the additional loads. Consequently, the licensee proposed to add the following equipment to the existing onsite ac and dc power systems as shown on Figures 4.2 and 4.3 of this SER supplement:

(1) two EDGs (Transamerica Delaval, Inc., TDI)

(2) two trains of independent Class 1E 4160/480-V electric distribution, each with an independent load sequencer

(3) four trains of independent Class 1E 125-V dc power with the associated batteries, primary and standby chargers, and 120-V ac vital instrument power supplies

To house this new equipment, the licensee constructed two new Category I structures: a diesel generator building and a nuclear service electrical building (NSEB).

4.7.1 TDI Diesel Generator Qualification

4.7.1.1 Diesel Generator Requalification

Following a TDI diesel generator crankshaft failure at the Shoreham Nuclear Power Station and other problems with engine quality, the utility industry organized a TDI Owners Group to address TDI diesel reliability. This group, after extensive review, developed a corrective action program to be implemented before and after placing the TDI diesels into nuclear service. A site implementation plan was developed to implement this program at Rancho Seco in three basic phases. Phase A involved a pre-run engine teardown. Phase I involved preliminary diesel engine runs and tests (before phase B), and later, preoperational testing (after phase B). The third phase was phase B, which involved additional engine teardowns for wear and clearance inspections after preliminary engine runs.

Phase A engine inspections and part replacements were performed before initial engine runs to ensure that conditions and materials were satisfactory to prevent possible engine damage. This phase of the test program addressed the 16 known generic problem areas identified by the owners group program along with various other areas of concern. These areas were addressed using the licensee's Construction Inspection Data Report (CIDR) format. The phase A teardown occurred from November 1984 to February 1985. As a result of these phase A inspections, all engine piston skirts were replaced along with various bolting hardware

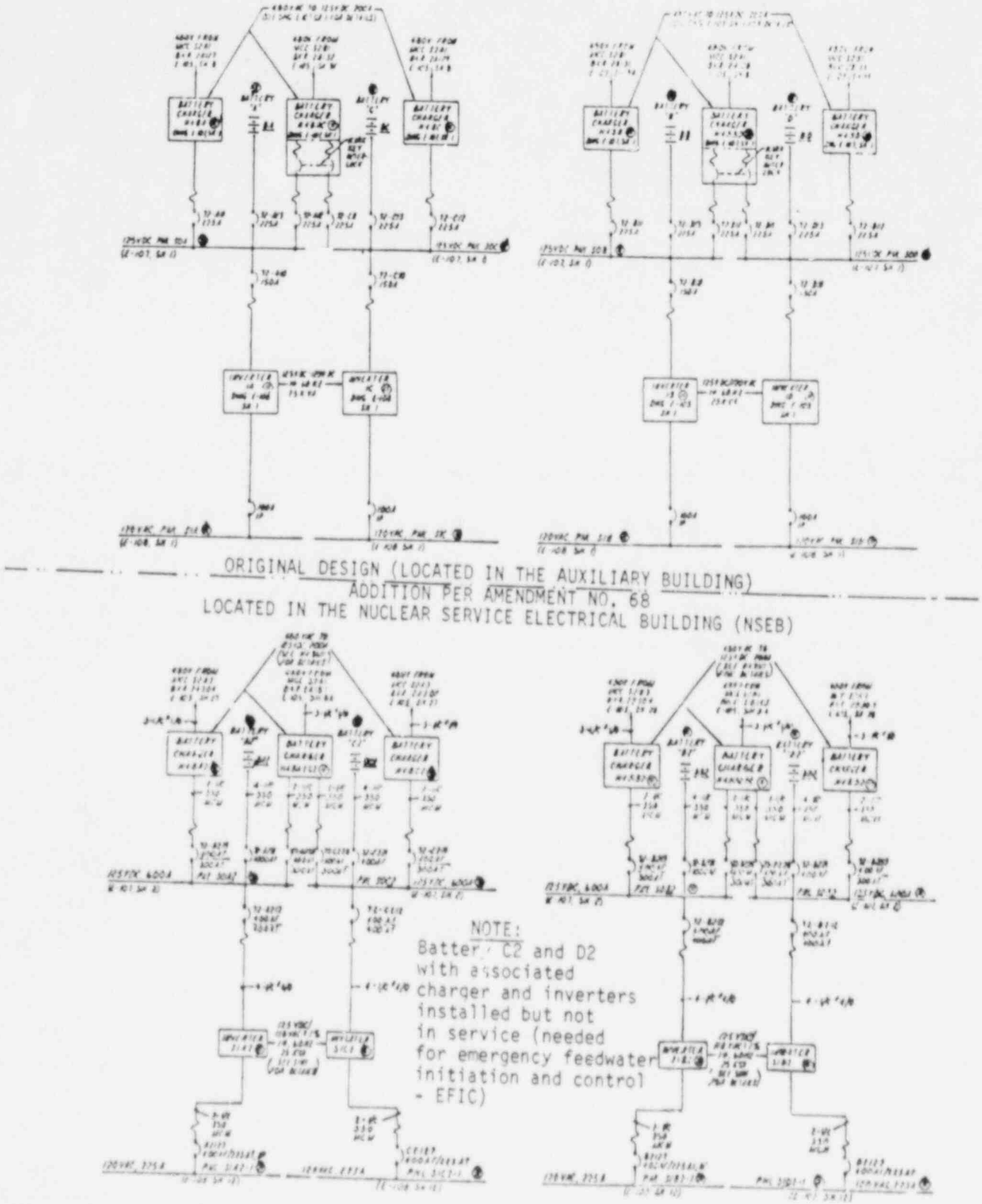
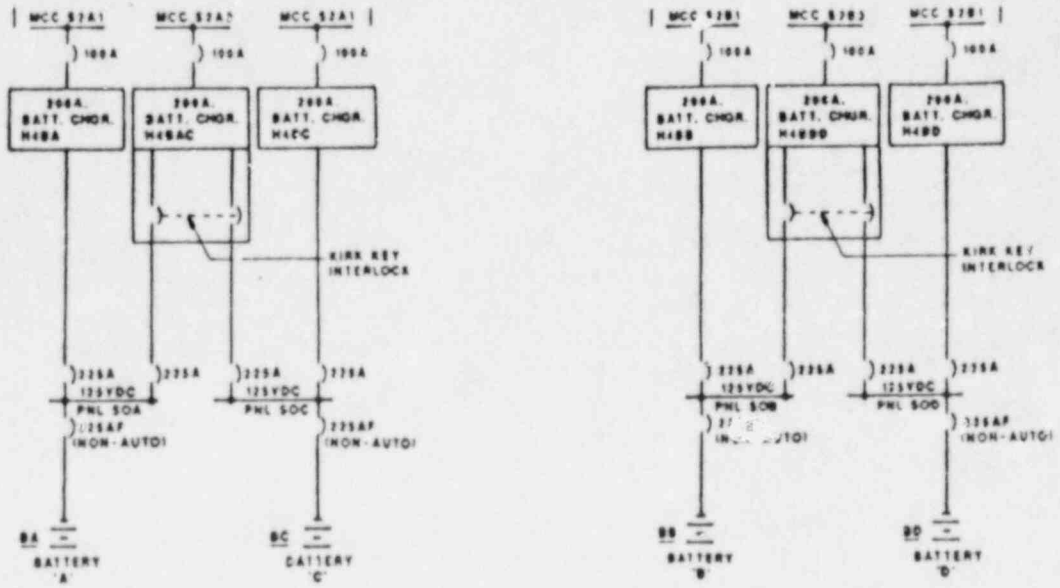


Figure 4.2 Rancho Seco Class 1E 125-V dc system and associated ac equipment



125VDC BATTERIES A, B, C AND D AND ASSOCIATED EQUIPMENT

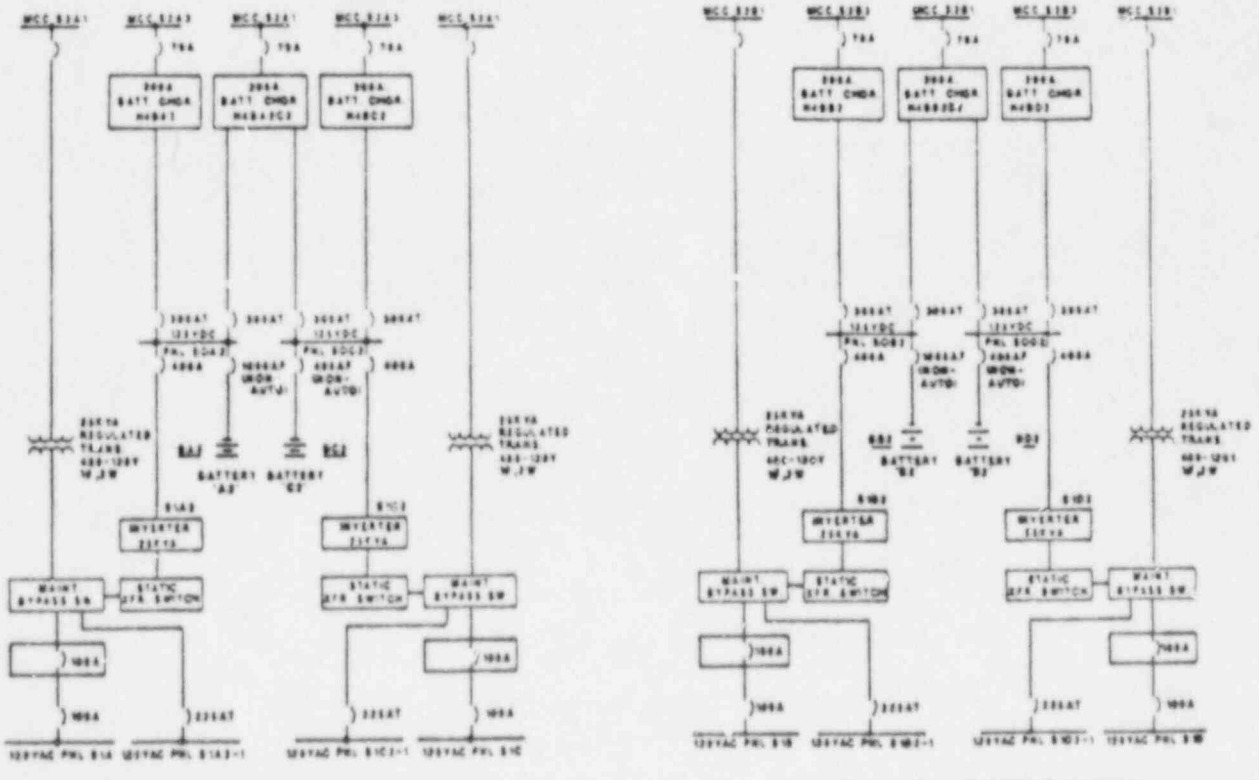


Figure 4.3 Rancho Seco Class 1E 125-V dc system and associated ac equipment (final design per Amendment 147)

on the turbocharger, flywheel, and engine. Several engine bearing shells were replaced because they did not meet minimum radiographic acceptance criteria. Rust and dirt were removed from the turbocharger during a disassembly inspection. Full details of the phase A engine work are contained in the partial Rancho Seco final Design Review/Quality Revalidation (DR/QR) Report submitted to the NRC on July 8, 1987.

After the phase A teardown work was completed, the individual diesel support systems (jacket water, fuel oil, starting air) on piping, mechanical, electrical and instrumentation components were tested. Initial electrical checks were performed on motor control centers (MCCs) and distribution panels, and component motors and the diesel control panels were tested. Individual components were tested mechanically, and all diesel piping systems were cleaned and flushed. Also, during this time period (March 1985 through July 1985), instrumentation and control logic was checked and calibrated.

This testing was a prerequisite to initial engine runs under Special Test Procedure (STP) 195A and B. The main purposes of STP 195A and B were as follows:

(1) Demonstrate automatic operation of the diesel generator system pumps, fans, and heaters.

(2) Demonstrate automatic operation of the diesel starting air system and satisfactory engine and component operating temperatures and pressures.

(3) Verify all system alarms and diesel trips and verify the capability of each air receiver tank to provide enough air for five consecutive cold starts.

(4) Demonstrate that the generator can be manually synchronized and paralleled with a temporary load transformer and that rated voltage is maintained during load shedding with no engine overspeeds.

(5) Obtain a minimum of 100 hours' run time at >50% load (>1750 kW) and demonstrate satisfactory operation of the diesels at 110% nameplate load (3850 kW) for 2 hours and 100% load (3500 kW) for 22 hours during a continuous 24-hour run.

(6) Perform torsiograph and vibration testing of the diesel generators and associated piping and components for baseline information.

These test objectives were met as documented with the final STP 195A/B test results. Testing took place from October through December 1986. After initial engine operations, the TDI Owners Group Maintenance Matrix (from the DR/QR Report) was placed into effect. Also, periodic lube oil testing was begun which included ferrographic analysis.

The following major problems were discovered and addressed as a result of STP 195A/B testing:

(1) Slow response time on the Woodward governor allowed overspeed trips when switching between electrical control and mechanical governor control. This was resolved by changing the governor oil to a type that has a broader temperature range for operation.

(2) Lube oil pump noise and vibration on the A engine was initially thought to be caused by out-of-specification lubricating oil. Oil samples were tested by TDI, Herguth Laboratories, and Mobil Oil Corporation, and met all specification requirements. During investigation, a nut was found lodged in the engine-driven lubricating oil pump suction foot valve which did not allow the valve to be fully open during operation. This foreign object was removed, resulting in a reduced level of noise and vibration, and engine testing continued.

(3) During testing, the engine vibration baseline and torsiograph test was performed, as required by the TDI Owners Group. The torsiograph testing results were analyzed, resulting in a proposed qualified load of 3300 kW. However, various piping vibration problems and turbocharger vibration problems were uncovered. The resolution of these problems is detailed in a separate report. This report will be submitted to the NRC and the staff will evaluate the issue before restart.

After initial diesel testing under STP 195A/B was completed, the phase B engine teardown was performed. The purpose of this teardown was to verify proper engine part clearances and to inspect for adverse wear after more than 100 hours of loaded operation. This teardown occurred from December 1986 through February 1987. The most important results are listed below.

(1) Because of excessive vibration during tests, the turbochargers were disassembled to inspect for bearing wear. Inspection revealed unsatisfactory bearing wear and the units were returned for rework. It was discovered that the rotors were out of balance; that condition was corrected before reinstallation Additional details for this component (MP-020) are contained in the licensee's final DR/QR Report submitted January 4, 1988.

(2) Several fuel injection pumps were replaced because of internal discontinuities and stuck rack extension arms.

(3) The engine-driven fuel oil pump was replaced because of excessive casing wear caused by an internal alignment problem.

(4) Several rocker arm assemblies were replaced because push rod cup holder bores were out of tolerance.

(5) Major design improvements were added to the fuel oil system by installing double-walled, high-pressure injection tubing with a visible leak and detection system from the pump outlets to the injectors. Also, high-temperature/pressure flex lines were installed from the fuel oil header to the injection pump inlet and from the pump excess flow port to the bypass return line. These modifications improved the integrity of the system pressure boundary.

Full details of phase B teardown results are documented in the Rancho Seco final DR/QR Report submitted to the NRC by letter of January 4, 1988.

In parallel with the phase B teardown, numerous piping and component vibration problems were addressed by support redesign and installation. These concerns are addressed in detail in the "Report of the Resolution to Vibration Related Concerns on the TDI Emergency Diesel Generators." As required in NUREG-1216,

an alarm circuit designed to notify control room operators when the diesel generators exceed "qualified load" was designed and installed during this time period. Also, engine base metal samples were analyzed for graphite and found to meet TDI Owners Group recommendations.

Following phase B teardown and new support installations for vibration attenuation, final preoperational testing was performed under STP 1009A/B. The main purposes of these tests were:

(1) Demonstrate diesel generator reliability by successfully completing 35 valid test starts per engine.

(2) Demonstrate that diesel generator maintains rated voltage after rejection of 3000 kW and that no engine overspeed trip occurs.

(3) Perform a 24-hour diesel generator run at 3000 kW.

(4) Verify that the internal temperatures of diesel generator control panels do not exceed design parameters while at 3000 kW for 24 hours.

(5) Demonstrate diesel operation, including voltage and frequency control, from the remote controls in the main control room.

(6) Demonstrate that the diesel engine automatically starts after the receipt of a simulated engineered safety features actuation system (ESFAS) signal, generates rated voltage and frequency, and is ready to accept load, within 10 seconds.

(7) Demonstrate the diesel capability to operate for a period of time with no load, and then assume full load without shutdown or adverse effects.

(8) Demonstrate that diesel generators can be manually synchronized and paralleled with the associated preferred offsite power supply through the associated Class 1E 4160-V bus, and can be loaded.

These test objectives were met as documented with the final STP 1009A/B test results. Testing was performed from April through August 1987. The following major problems were discovered and addressed as a result of this testing.

(1) Woodward governor response time and stability continued to be a problem. Governor hydraulic oil was switched to automatic transmission fluid (ATF) to alleviate this problem. While making this change, excessive metal filings and dirt were found in the governor internals. The units were removed and shipped to the governor vendor (Woodward Governor Co.) for cleaning, inspection, and repair as required. Also, the servoboosters were inspected and cleaned along with the governor heat exchangers. Upon their return from the vendor, the governor components were verified to be clean before installation and ATF was used as hydraulic oil. The governors performed satisfactorily during continued testing both in response time and sensitivity.

(2) After a 24-hour loaded diesel run, a simulated ESFAS signal was generated, but the diesel did not start for approximately 90 to 120 seconds.

This delay in start time was corrected by a TDI (vendor-supplied) design change to allow for an immediate restart instead of waiting 90 seconds. The change was made and tested satisfactorily.

(3) The retest of various piping and components indicated that some modifications to resolve vibration concerns were successful, and others were inadequate. Once again, these are detailed in "Report of the Resolutions to Vibration Related Concerns on the TDI Emergency Diesel Generators," which report will be evaluated by the NRC staff. The staff's evaluation of the TDI vibration report will be documented in Section 4.7.1.2 of a future SER supplement, or in another appropriate document, such as a letter to the licensee.

Diesel generator reliability will be improved by adherence to the TDI Owners Group enhanced Maintenance Matrix Program and a detailed maintenance and surveillance test program as discussed in Section 4.7.1 of the restart SER. These programs, coupled with the extensive requalification test effort, will ensure reliable TDI diesel generator operations at Rancho Seco in support of plant power operations.

4.7.1.2 TDI Diesel Generator Vibration Problems Resolution

The staff's evaluation of the resolution of the TDI diesel generator vibration problems will be addressed in a separate appropriate document before restart.

4.7.2 Emergency Diesel Generators and Supporting Auxiliary Systems

This discussion is confined to the two diesel generators that were recently installed and their supporting auxiliary systems. The diesel generators that were in place when the plant was originally licensed, including their auxiliary systems, will not be readdressed in this supplement.

Each of the two new diesel generators has the auxiliary systems listed below. These systems are discussed in detail in the sections indicated in parentheses after the system name.

(1) fuel oil storage and transfer system (4.7.2.2)
(2) cooling water system (4.7.2.3)
(3) starting system (4.7.2.4)
(4) lubrication system (4.7.2.5)
(5) combustion air intake and exhaust system (4.7.2.6)

The design of the diesel generator auxiliary support systems also has been evaluated with respect to the recommendations of NUREG/CR-0660, "Enhancement of On-site Emergency Diesel Generator Reliability." This report made specific recommendations on increasing the reliability of nuclear plant emergency diesel generators (EDGs). Conformance of the licensee's design to these recommendations is shown in Table 4.5.

The diesel generator design will conform to the requirements of GDC 2, 4, 5, 17, 18, and 21 and the applicable RGs and industry standards. The design of the diesel generators and their auxiliary systems will then also be in conformance

Table 4.5 Licensee's conformance to the recommendations of NUREG/CR-0660

Recommendation		Conformance
1.	Moisture in air starting system	Yes
2.	Dust and dirt in diesel generator room	Yes
3.	Turbocharger gear drive problem	N/A
4.	Personnel training	Yes
5.	Automatic prelube	Yes
6.	Testing, test loading, and preventive maintenance	Yes
7.	Improve identification of root cause of failures	Yes
8.	Diesel generator ventilation and combustion air systems	Yes
9.	Fuel storage and handling	Yes
10.	High-temperature insulation	*
11.	Engine cooling water	Yes
12.	Concrete dust control	Yes
13.	Vibration of instruments	Partial

*The staff considers explicit conformance unnecessary in view of the equivalent provided by the design, margin, and qualification testing requirements that are normally applied to emergency standby diesel generators.

with the recommendations of NUREG/CR-0660 for enhancement of diesel generator reliability.

4.7.2.1 New TDI Emergency Diesel Generator Design and Test Capability

The design and test capability of the new EDGs were reviewed to establish compliance with the applicable GDCs (GDC 2, 4, 17, and 18), regulatory guides (RGs 1.6, 1.9, 1.108), Branch Technical Position (BTP) ICSB 8, and IEEE Standard 323-1974.

The new TDI EDG has a nominal capacity rating of 3500 kW and is designed to withstand 10% overload for at least 2 hours out of every 24 hours of operation and is also capable of operation at low loads for extended periods without degradation. As a result of the TDI generic issue, the EDG has been requalified to supply a 3300-kW continuous load. The safety loads on each redundant train will be supplied by two independent diesel generators. The loads on the old EDG (Bruce GM) and the new EDG (TDI) are so distributed that any combination of two EDGs (one old and one new on either of the two trains) can provide power to safely shut down the plant given the design-basis accident. The load margin available for future addition of loads is 51% and 24% of the engine rating in the new and old EDGs, respectively.

The new EDGs are located in a new quality assured seismic Category I diesel generator building, and their associated engine and generator control panels are located in rooms separate from the EDGs themselves. The EDGs and control

panels are seismically qualified. Each EDG is automatically started by an engineered safety feature actuation signal (ESFAS) or a loss-of-offsite-power (LOOP) signal and will be connected to its associated bus following a loss of voltage to the bus. The loss of bus voltage signal is bypassed after the EDG breaker is closed. The EDGs can be monitored and controlled from the main control room or locally. Additionally, the controls of the new EDG in one redundant train can be isolated from the main control room by means of a switch located in the NSEB to provide an alternate emergency control capability in case of a control room fire. The dc power source for each new EDG control and instrumentation is from the same train as the EDG and its associated switchgear. To supply power to the EDG support (auxiliaries) ac components, the licensee has added motor control centers (MCCs) (two for each EDG) on the 480-V ac load center buses associated with each EDG. Regarding the SRP comparison (Section 8.3.1.III.6), the licensee stated that the design of these MCCs will meet the same independence, redundancy, and separation requirements as their associated EDG system and the specific design requirements of the electrical distribution system licensed by Amendment 68.

In response to the staff's questions regarding voltage, frequency, bypass circuits, tests, and qualification of the proposed TDI EDGs, the licensee submitted its response (letters dated April 1 and October 30, 1987) that the installed EDGs meet the qualification requirements of IEEE Standard 323-1974 and RG 1.100, the design requirements of the RG 1.9, and testing requirements of RG 1.108 and GDC 18.

Position 7 of RG 1.9, "Selection, Design, and Qualification of Diesel-Generator Units Used as Standby (Onsite) Electric Power Systems at Nuclear Power Plants," Revision 2, allows engine overspeed and generator differential to trip the diesel generator by a single channel trip. All other diesel generator protective trips are to be implemented with two or more independent measurements for each trip parameter with coincident logic, or bypassed under accident conditions, provided the operator has sufficient time to react appropriately to an abnormal condition of the diesel generator. The licensee is retaining engine overspeed and generator differential with a single channel trip and low lubricating oil pressure with coincident logic during an accident, and bypassing all other protective trips, maintaining that the operator has sufficient time to respond to an alarm for an abnormal condition.

As shown in Figure 4.2 of this supplement, the A2 train is powered from startup transformer No. 1 and the B2 train is powered from startup transformer No. 2. Electrical interlocks permit testing of A train diesel generators through startup transformer No. 1 only and of B train diesel generators through startup transformer No. 2 only. Regarding compliance to BTP 8 and RG 1.6 requirements, the licensee has committed in proposed Amendment 147 not to use the EDGs for commercial power production.

Only one of the four EDGs can be tested at a time, using administrative procedure (keylock arrangement for the selector switches) to prevent interaction of the EDGs within and between the redundant trains. However, the test setup design uses one synchroscope which can be connected through selector switches to the potential transformers on the buses, EDGs, and offsite power sources in both trains. A single failure in the selector switches associated with an EDG in one train, while its counterpart in the redundant train is being synchronized

with its associated offsite source of power, could cause redundant EDG potential transformers to parallel and cause blowing of fuses or relays energizing redundant EDG instrumentation circuits. The licensee's response to this concern is documented in the previously cited letters of April 1 and October 30, 1987. It provides a failure modes and effects analysis which concludes that even a complete failure of any of the several selector switches will not result in paralleling of redundant division EDGs. For the scenario identified in the staff's question, the licensee stated that the voltage balance relays associated with the EDGs will be energized to cause EDG control circuit lockout and "DG inoperative" alarm in the EDG rooms and the main control room. The staff found the licensee's response acceptable and has concluded that the postulated failure would not result in paralleling or otherwise compromise redundant EDGs power sources.

SRP Section 8.3.1.4.f(3) requires the licensee's preventive maintenance program to encompass investigative testing and replacement plan. The licensee has informed the staff in the letters of April 1 and October 30, 1987 that the Rancho Seco maintenance and preventive maintenance program will comply with the requirements of NUREG-1216, "Safety Evaluation Report Related to The Operability and Reliability of Emergency Diesel Generators Manufactured by Transamerica Delaval, Inc." This NRC document includes the required investigative testing and replacement plan for TDI emergency diesel generators, and the program is, therefore, acceptable.

The staff's review of the design information provided with proposed Amendment 147 reveals that the EDG design complies with GDC 2, 4, and 17 and meets the requirements of RG 1.6 and BTP 8. Compliance of the new EDG installation, power, control, and instrument circuits to the requirements of RG 1.75 was addressed in the SER (NUREG-1286) issued in October 1987. The EDG auxiliary and support systems design, except for RG 1.75 considerations, were evaluated in Sections 4.7.2.2 through 4.7.2.6 of this supplement (SSER 1). The design information provided with proposed Amendment 147 did not specifically address compliance to the regulatory positions of RG 1.9 and 1.108 and did not include the qualification documents to establish compliance to RG 1.100 and IEEE Standard 323-1974. However, in response to staff questions, the licensee has committed to comply with these regulatory positions. Based upon its evaluation of the information provided to the staff and the licensee's commitment for design compliance to the NRC regulatory positions, the staff concludes that the proposed design and test capability of the electrical aspect of the EDGs is acceptable.

4.7.2.2 Diesel Engine Fuel Oil Storage and Transfer System

The design function of the emergency diesel engine fuel oil storage and transfer system is to provide a separate and independent fuel oil supply train for each diesel generator and to permit operation of the diesel generator at ESF load requirements for a minimum of 7 days without replenishment of fuel. The system is designed to meet the requirements of GDC 2, 4, 5, and 17.

Each new diesel engine fuel oil storage and transfer system consists of a 550-gallon day tank sufficient to power the diesel engine at a continuous-rated load for approximately 2 hours, a 60,000-gallon diesel fuel oil storage tank sufficient to power the diesel engine based on the continuous-rated load for in

excess of 7 days, two ac motor-driven transfer pumps, and associated piping, valves, instrumentation, and controls.

Except as noted below, the diesel engine fuel oil storage and transfer system is independent of and physically separated from the other system supplying the redundant diesel generator. Thus, a single failure within any one of the systems will affect only the associated diesel generator. The single exception is the cross-tie between the discharges of the fuel oil transfer pumps. This cross-tie allows fuel from one storage tank to be delivered to either or both day tanks, depending on the alignment of specific valves in the respective fuel oil systems. In normal operation, the manual valves in the cross-tie are locked closed. Since the manual valves are not active components, they are not subject to failure, and the independence of the fuel oil storage and transfer systems is not compromised. Except for the flame arrestors on the storage tank and day tank vent lines, the fuel oil storage and transfer system piping and components up to the diesel engine interface are designed to seismic Category I, ASME Code Section III, Class 3 (Quality Group C) requirements. They meet the recommendations of RG 1.26, "Quality Group Classifications and Standards for Water-, Steam-, and Radioactive-Waste-Containing Components of Nuclear Power Plants," and RG 1.29, "Seismic Design Classification." The engine-mounted piping and components, from the engine block to the engine interface, are considered part of the engine assembly and are seismically qualified to seismic Category I requirements as part of the diesel engine package.

During its review, the staff requested that the licensee show how it would minimize fuel oil degradation that could result from turbulence of sediment in the bottom of the fuel oil storage tank during the addition of new fuel. The licensee response was that the cross-tie between systems could be manually activated to supply fuel oil to both engines from one storage tank while the other storage tank was being filled and the sediment could be allowed to settle. The staff finds this acceptable because use of the cross-tie for the above purpose has been included in the appropriate plant operating procedures.

The basis for acceptance in the staff review was conformance of the design criteria and bases and design of the diesel engine fuel oil storage and transfer system to the requirements of GDC 17 with respect to redundancy and physical independence, to the guidance of the cited RGs, to the recommendations of NUREG/CR-0600, and to industry codes and standards.

On the basis of its review, the staff concludes that the emergency diesel engine fuel oil storage and transfer system meets the requirements of GDC 2, 4, 5, and 17 and meets the recommendations of NUREG/CR-0660, the guidance of the cited regulatory guides and SRP 9.5.4, and industry codes and standards, and can perform its design safety function. The staff concludes, therefore, that the design of the fuel oil storage and transfer system is acceptable.

4.7.2.3 Diesel Engine Cooling Water System

The design function of the emergency diesel engine cooling water system is to maintain the temperature of the diesel engine within a safe operating range under all load conditions and to maintain the engine coolant preheated during standby conditions to improve starting reliability. The system is designed to meet the requirements of GDC 2, 4, 5, 17, 44, 45, and 46.

The closed-loop system provides cooling for the engine jacket, engine lubricating oil, governor oil, the turbocharger, and combustion air. During operation of the diesel generators, the temperature of the diesel engine coolant is regulated automatically through the action of a temperature-sensing three-way thermostatic valve. When the diesel generator is idle, the engine coolant is heated by an electric heater and continuously circulated through the engine. The temperature is controlled by a thermostat to keep the engine warm and ready to start and accept loads within the prescribed time interval.

Each radiator has six fans to draw air across the cooling surfaces. The fans are powered from a Class 1E source which, in turn, is powered by the diesel generator associated with that radiator. The diesel generators can operate without air flow across the radiators for a long enough period to allow sequencing the fans on without overheating.

The coolant in the diesel generator cooling systems is treated to prevent corrosion and fouling, and a blend of water and antifreeze solution protects against freezing without impairing heat transfer. Each diesel generator has a physically separate and independent cooling water system, so the requirements of GDC 17 and 44 with regard to redundancy and the single-failure criterion are met.

The diesel generator cooling water system piping and components up to the diesel engine auxiliary skid are designed to seismic Category I, ASME Code Section III, Class 3 (Quality Group C) requirements and meet the recommendations of RGs 1.26 and 1.29. Piping and components on the auxiliary skid are designed to ANSI Standard B31.1 augmented to include material traceability. The auxiliary skid-mounted piping and components are overdesigned (subjected to low working stress for the application), thereby resulting in high operational reliability. The engine-mounted piping and components, from the engine block to the engine interface, are considered part of the engine assembly and are seismically qualified to seismic Category I requirements as part of the diesel generator package.

The diesel engine cooling water system has provisions to permit periodic inspection and functional testing during standby and normal modes of power plant operation as required by GDC 45 and 46.

The bases for the acceptance in the staff review were (1) conformance of the design criteria and bases and design of the diesel engine cooling water system to GDC 17 and 44 with respect to redundancy and physical independence, to GDC 45 and 46 with respect to inspection and testability of the system, to the guidance of the cited regulatory guides, and to the recommendations of NUREG/CR-0660 and industry codes and standards, and (2) the ability of the system to maintain stable diesel engine cooling water temperature under all load conditions.

On the basis of its review, the staff concludes that the emergency diesel engine cooling water system meets the requirements of GDC 2, 4, 5, 17, 44, 45, and 46; meets the guidance of the cited regulatory guides and SRP Section 9.5.5; and meets the recommendations of NUREG/CR-0660 and industry codes and standards, and is therefore acceptable.

4.7.2.4 Diesel Engine Starting System and Backup Air System

The design function of the emergency diesel engine starting system is to provide a reliable method for automatically starting each diesel generator so that the rated frequency and voltage are achieved and the unit is ready to accept required loads within 10 seconds. The system is designed to meet the requirements of GDC 2, 4, 5, and 17.

Each new diesel generator has an independent air starting system sized to provide for 10 consecutive diesel generator starts without recharging. The air starting system for each diesel generator consists of an ac-motor-driven air compressor, a cooler, an air dryer, two air receivers, piping and valves to connect the components to each other and the system to the diesel generator, and system controls. The piping and valves are arranged so that a failure of one air receiver will not cause a loss of air in the other receiver with attendant loss of diesel generator starting capability. The air starting system for each diesel generator is totally independent of the starting system for the other diesel generator and there is redundancy within each air starting system, so the requirements of GDC 17 are met.

The engine-mounted piping and components, from the engine block to the engine interface, are seismically qualified to seismic Category I requirements as part of the diesel generator package.

Piping and components within the air starting systems from the compressor up to the check valve on the inlet of each air receiver are non-safety, seismic Category II. From the air receiver check valves to the diesel engine interface, the piping and components are designed to seismic Category I, ASME Code Section III, Class 3, except as noted below. The air receivers themselves are designed to seismic Category I, ASME Code Section VIII, and the 1-inch drain valve on the drain line for each air receiver is designed to ANSI Standard B31.1 augmented to include material traceability and testing in accordance with ASME Code Section III, Class 3. This augmented ANSI standard is considered the equivalent of ASME Code Section III, Class 3 with regard to system functional operability and inservice reliability. In order to improve reliability for diesel engine starting and control air, the licensee has provided a backup air system, as described below.

The backup air system is a seismic Category I system which will provide air to the TDI pneumatic controls when air pressure in the TDI air receiver decreases to 75 psig. Backup air use for 7 days of diesel operation is calculated to be 1569 standard cubic feet (scf). This value is based on observed engine air use during seismic testing. The six "active" bottles have a capacity of 161. scf. This figure is obtained assuming a starting pressure of 2400 psig at 70°F (300 scf/bottle) and a final pressure of 100 psig (13.4 scf/bottle). The "backup bottle low air pressure" alarm setpoint of 150 psig provides 2 hours' operation before the 100-psig minimum pressure is reached. A relief valve is set at 275 psig to prevent overpressurizing the existing TDI air system lines.

During normal operation, air to pneumatic control is provided by the existing TDI air receivers. Normal pressure in the air starting system is approximately 250 psig. A pressure control valve in each TDI air system provides service from the backup air supply. The pressure control valve will not allow flow

from the backup air bottles until system pressure downstream of the valve decreases to 75 psig; the pressure control valve then modulates to maintain system pressure at 75 psig. The six "active" backup air bottles provide sufficient air for seven days' operation, with six "reserve" backup air bottles for emergency or extended use. Isolation valves and check valves are provided in the backup air system for system isolation and to prevent back flow, respectively.

The backup air system has been functionally tested to ensure it will supply air to the diesel air system for 7 days, and is acceptable to perform its intended function to supply backup air for starting and control of the emergency diesel generators.

Operating experience at two nuclear power plants has shown that during periodic surveillance testing of a standby diesel generator, initiation of an emergency start signal (LOCA or LOOP) resulted in the diesel failing to start and perform its function because repeated activation of the starting relay depleted the starting air supply. This event was noted in Information Notice 83-17. The licensee has reviewed that notice and the concern identified there, and has determined that the concern does not apply to the Rancho Seco configuration and procedures.

The bases for acceptance in the staff review were (1) conformance of the design criteria and bases and design of the diesel engine air starting system to the recommendations of NUREG/CR-0660 and to industry codes and standards, (2) the ability of the system to start the diesel generator within a specified time period, and (3) the ability of the system to maintain diesel generator operation subsequent to starting for an indefinite period of time.

On the basis of its review, the staff concludes that the emergency diesel engine air starting system meets the requirements of GDC 2, 4, 5, and 17, meets the guidance of the cited regulatory guides and SRP Section 9.5.6, the recommendations of NUREG/CR-0660, and industry codes and standards, and can perform its design function and is acceptable.

4.7.2.5 Diesel Engine Lubricating Oil System

The design safety function of the emergency diesel engine lubricating oil system is to provide a supply of filtered lubrication oil to the various moving parts of the diesel engine, including piston and bearings. The system is designed to meet the requirements of GDC 2, 4, 5, and 17.

The emergency diesel engine lubricating oil system is an integral part of the diesel engine and thus must meet the requirements of GDC 17 with regard to system independence and the single-failure criterion.

The lubricating oil heat is rejected to the diesel engine jacket water system. During engine operation, the engine-driven lubricating oil pump takes oil from the lubricating oil sump and delivers it under pressure to the engine moving part via the lubricating oil cooler. During standby, the engine prelubrication pump takes oil from the sump and delivers it under pressure to the lower part of the engine only (crankshaft, connecting rods, piston pins, and piston crowns). By design, no lubricating oil goes to the upper cylinder head area during standby, and only a very small amount is delivered to the turbocharger. This design precludes a buildup of excessive amounts of lubricating oil in the turbocharger

which could result in a fire, or in excessive amounts of oil on the cylinder heads that could drain into the cylinders and cause hydraulic lock. A thermostatically controlled heater maintains the oil temperature near operating temperature to enhance first-try starting reliability.

The lubricating oil system is mounted completely either on the engine itself, or on the diesel generator auxiliary skid. The auxiliary skid-mounted piping and components are designed to ANSI Standard B31.1, augmented to include material traceability. The auxiliary skid-mounted piping and components have also been pressure tested in accordance with ASME Code Section III, Class 3. The engine-mounted piping and components, from the engine block to the engine interface, are seismically qualified to seismic Category I as part of the diesel generator package.

The basis for acceptance in the staff review was conformance of the design criteria and bases and design of the diesel engine lubricating oil system to the requirements of GDC 17 with respect to redundancy and physical independence, to the guidance and additional acceptance criteria of SRP Section 9.5.7, to the recommendations of NUREG/CR-0660, and to the industry codes and standards.

On the basis of its review, the staff concludes that the emergency diesel engine lubricating oil system meets the requirements of GDC 2, 4, 5, and 17; the guidance of the cited regulatory guides and SRP Section 9.5.7; and the recommendations of NUREG/CR-0660 and industry codes and standards, and can perform its design safety function and is acceptable.

4.7.2.6 Diesel Engine Combustion Air Intake and Exhaust System

The design function of the emergency diesel engine combustion air intake and exhaust system is to supply filtered air for combustion to the engine and to dispose of the engine exhaust to the atmosphere. The system is designed to meet the requirements of GDC 2, 4, 5, and 17.

A separate source of combustion air for each diesel engine is taken from the associated diesel generator air intake damper through an air filter, turbocharger compressor, and combustion air coolers. The path of the exhaust gas discharge is through the turbocharger to the exhaust piping to the silencer located on the roof of the diesel generator building. The location of the combustion air intake and exhaust relative to each other precludes the possibility of recirculating exhaust gases and thereby degrading diesel generator performance.

There are no fire-extinguishing agents or noxious gases stored in the vicinity of air intakes which, if released, could cause diesel generator degradation or failure.

The diesel engine combustion air intake and exhaust system piping, excluding the intake filter and silencer, and the exhaust silencer, up to the diesel engine interface, is designed to seismic Category I, ASME Code Section III, Class 3 requirements. The engine-mounted piping from the diesel engine block to the engine interface are seismically qualified to seismic Category I as part of the diesel generator package. All essential components are seismic Category I, and the intake and discharge silencers are seismic Category I and Quality Class 1 design.

The bases for the acceptance in the staff review was conformance of the design criteria and design of the diesel engine air intake and exhaust system to GDC 17 with respect to redundancy and physical independence, to the guidance of the cited regulatory guides, to the guidance and additional acceptance criteria of SRP Section 9.5.8, to the recommendations of NUREG/CR-0660, and to industry codes and standards, as well as the ability of the system to provide sufficient combustion air and release of exhaust gases to enable the emergency diesel generator to perform on demand.

On the basis of its review, the staff concludes that the emergency diesel engine intake and exhaust system meets the requirements of GDC 2, 5, and 17 and meets the requirements of NUREG/CR-0660, the guidance of the cited regulatory guides and SRP Section 9.5.8, and industry codes and standards. Although the intake and exhaust system does not comply with the specific requirements of GDC 4 in that the exhaust silencers and part of the exhaust piping are exposed on top of the diesel generator building, the licensee's position on this is that no credible tornado missile that could render the exhaust system inoperable will occur at the elevation of the exhaust silencers. The staff has reviewed the tornado data for Rancho Seco and agrees with the licensee regarding tornado missiles and the exhaust silencers. Therefore, the staff concludes that the combustion air intake and exhaust system meets the requirements of GDC 4, can perform its design safety function, and is acceptable.

The preceding material applies to the combustion air intake and exhaust system, exclusive of the turbocharger itself. During testing, it was noted that the turbocharger on each emergency diesel generator (EDG) was vibrating excessively. An interim support to reduce vibration was installed to allow continued testing while a permanent solution was being designed. The turbocharger vibration problem has since been resolved with a permanent solution in place that has been tested. The more general subject of diesel generator vibration problems and their resolution will be addressed in a separate appropriate document before startup.

4.7.2.7 Conclusions, Emergency Diesel Generator and Supporting Auxiliary Systems

The staff evaluated the TDI emergency diesel generators and auxiliary supporting systems and finds these systems to be acceptable and the issue to be closed as a restart issue, except for the vibration problem as identified in Section 4.7.1.2.

4.7.3 Class 1E Electrical Distribution Systems Associated With the Diesel Generators

The SER related to the restart of Rancho Seco (NUREG-1286) addressed certain issues regarding Class 1E electrical distribution systems associated with the diesel generators. Although the first four issues (Sections 4.7.3.1 through 4.7.3.4) were closed as restart issues, the "Conclusions" to Section 4.7.3 (SER Section 4.7.3.5 and SER Supplement 1 Section 4.7.3.8) state that the staff is reviewing other electrical aspects of the TDI diesel generators at Rancho Seco. These are addressed below (Sections 4.7.3.5 through 4.7.3.7).

4.7.3.1 Equipment Separation

This was found to be acceptable and was closed as a restart issue in NUREG-1286.

4.7.3.2 Raceway Separation

This was found to be acceptable and was closed as a restart issue in NUREG-1286.

4.7.3.3 Internal Separation

This was found to be acceptable and was closed as a restart issue in NUREG-1286.

4.7.3.4 Raceway/Circuit Identification

This was found to be acceptable and was closed as a restart issue in NUREG-1286.

4.7.3.5 120-Volt ac Vital Instrument Power Systems Uninterruptible Power Supply Modification

The purpose of this modification is to improve the reliability of the vital 120-V ac power supplies. As shown on Figure 4.2 of this supplement, the design of 120-V ac vital power systems consisted of the four, inverter-supplied, 120-V ac buses in the auxiliary building (original design) and a similar set of four buses in the nuclear service electrical building (additions in response to NUREG-0737 and NUREG-0696). The licensee's proposal in proposed Amendment 147 changes the present configuration as shown on Figure 4.3 of this supplement. As a result of the modifications, the 120-V ac vital buses in the auxiliary building will be disconnected from their associated inverters which were found to be unreliable. Because they have experienced several recent failures and found it difficult to obtain replacement parts (the vendor of these inverters has gone out of business), these inverters are being removed from the plant. Their associated 120-V ac vital buses in the auxiliary building will be supplied by the recently added NSEB inverters as shown on Figure 4.3. In essence, the existing eight-inverter/eight-bus system will be modified into a four-inverter/ eight-bus system. Each of the four inverters is rated 25 KVA. The maximum combined two-bus load on any one inverter will be less than 15.2 KVA.

The proposed modification also includes a seismically qualified Class 1E static transfer switch and a manual bypass switch with each of the four inverters. The function of the transfer switch is to immediately and automatically transfer the 120-V ac vital bus load to a backup source of 120-V ac regulated power in case of a loss of its associated inverter. The design is such that each of the two uninterruptible power supplies (UPSs) in one train is backed up by both EDGs in that train. If one EDG in a train fails, or both primary and backup chargers supplying an inverter fail, or the inverter itself fails, the static transfer switch will automatically switch both of the associated UPS buses over to the other EDG in that train. If both EDG supplies to any one of the two associated UPS in a train fail, the affected UPS will operate from its associated battery for at least 2 hours. The function of the manual bypass switch is to ensure that 120-V ac regulated power is available to the UPS buses when the associated inverter and the static transfer switch have failed or are out for maintenance.

The staff's review of the licensee's submittal indicates that the proposed design of the 120-V ac vital instrument power has the required redundancy with sufficient capacity and adequate capability to provide the design safety function. The design is testable in accordance with the periodic testing requirement of GDC 18. The physical and electrical independence of the modification

was previously reviewed by the staff and the findings were provided in the Rancho Seco Restart SER. The staff concludes that the proposed modification meets the redundancy, capacity, capability, and testability requirements of GDC 17 and thus is acceptable.

4.7.3.6 4160-Volt ac Class 1E Bus Overvoltage/Undervoltage Alarm and Trip Relaying Scheme Modification

At Rancho Seco, the existing schemes for alarming and tripping an abnormal offsite power to protect the Class 1E electric equipment from overvoltage and undervoltage was implemented in response to an NRC letter to the licensee dated June 3, 1977. This letter required all plants to have a second level of undervoltage or overvoltage protection. The licensee did not rely on operator action for overvoltage protection and proposed to implement automatic protection from undervoltage as well as from overvoltage. The proposed scheme included one relay for overvoltage alarm and three relays in a 2-out-of-3 coincident logic on each 4160-V Class 1E bus for overvoltage trip. Similarly there are three relays on each 4160-V Class 1E bus to provide undervoltage trip (combined loss of voltage and degraded grid voltage) in a 2-out-of-3 coincident logic. Both undervoltage and overvoltage protection schemes were reviewed and approved by the staff in letters dated December 4, 1980 and August 10, 1983.

In the recent past, the plant experienced spurious overvoltage tripping due to transient overvoltages associated with reactor coolant pump (RCP) starting or high grid voltages of short duration. The RCPs are supplied by one winding of the startup transformer; the Class 1E buses are supplied from the other winding. The transformer is designed so that when low voltage occurs on one winding during RCP start, voltage compensation causes higher voltage on the other winding (to Class 1E buses). This increase in voltage exceeds the overvoltage, 8-second, time delay, trip setpoint and causes the bus to trip from the offsite source of power and the consequential start of the EDGs. To prevent this unnecessary challenge to the emergency ac power systems, the licensee has proposed to eliminate the overvoltage trip and to implement operating procedures to limit 4160-V engineered safety features (ESF) bus voltage within the acceptable range. If the operator cannot reduce the overvoltage to the normal operating range of the 4160-V Class 1 bus after the alarm, then the operator must start the diesel generator, parallel it with the offsite source, reduce the load on the 4160-V ESF bus to the allowable limit of diesel generator loading, and then trip the offsite power circuit breaker.

The modification to the overvoltage alarm design is to replace the existing alarm relay with a voltage transducer to provide analogue signals for logging and alarming the 4160-V ESF bus overvoltages at the plant computer (interim data acquisition and display system, IDADS) located in the main control room.

The staff finds the alarm modification acceptable. However, the operator action to parallel EDGs with an abnormal offsite power source, and operating the EDGs to assume loads from the higher voltage offsite power supply, has a potential for common mode failure, an unacceptable condition. The licensee did not include any justification as to why the time delay for overvoltage trip should not be increased from its present value of 8 seconds to accommodate the RCP starting transient and continue to provide the required automatic overvoltage protection. The proposed operator action would override the transient and would only be applicable in the case of sustained overvoltage on the offsite power system.

The sustained overvoltage of the offsite power would be due to grid overvoltage and would affect all four 4160-V ESF buses. In response to the staff's concern, the licensee has committed (letters dated April 1 and October 30, 1987) to not parallel the EDGs with the offsite source of power except for testing. The offsite power supply breakers to the 4160-V Class 1E buses will be tripped before the bus voltage reaches its analyzed limit of 4626 V. This is in compliance with BTP ICSB 8 which requires precluding interconnection of onsite and offsite power sources, except for short periods for the purpose of load testing. The staff finds the licensee's proposal acceptable.

In the Rancho Seco design, both loss of voltage trip and the degraded grid undervoltage trip were provided by the same set of inverse characteristic undervoltage relays. The trip setpoint for these undervoltage relays was chosen to protect Class 1E electrical equipment from harmful undervoltages during all plant operating conditions and transients. The trip setpoint provided in the Rancho Seco technical specifications is 3771 ± 38 V on the 4160-V nominal voltage base and the tested relay operating characteristic is to drop out within 8.2 ± 0.82 second at 98% of the setpoint, within 5.2 seconds ± 0.52 second at 90% of the setpoint, within 3.1 seconds ± 0.31 second at 70% of the setpoint, and within 1.5 seconds ± 0.15 second at zero volts (0 V).

However, the relay operating accuracy is not predictable because the inverse operating characteristic of the relay does not accurately repeat for certain voltage zones of the relay operation. The licensee experienced unpredictable drifts in the relay operation, thus causing noncompliance with the technical specification limits. The licensee's proposed modification is to provide a set of definite time delay undervoltage relays in a 2-out-of-3 trip logic in conjunction with the existing inverse characteristic undervoltage relays. The inverse characteristic relays will be used for first level of protection (loss of offsite power) to drop out at 70% of the trip setpoint with a time delay of 3.5 seconds. At or below this voltage, the operating characteristic of the inverse relays is well defined and the setpoint repeatability is predictable. The definite time delay relays will be used for the second level of protection (long time undervoltage due to degraded grid) to drop out at 98% of the trip setpoint with a time delay of 5 seconds ± 0.5 second. Both relays are set to trip at the existing setpoint of 3771 V ± 38 V. With this selection of time delays, the definite time delay relay will always operate faster than the inverse characteristic relays above 90% of the undervoltage trip setpoint. This design will eliminate dependence on the inverse characteristic relays for their operation in the steep portion of the time delay curve where the setpoints are not accurately repeatable. The staff has reviewed the time delay curves given in the licensee's letters of April 1 and October 30, 1987, and agrees with the licensee's approach.

The new relays and their associated cables and raceways will be qualified for their Class 1E function and will be tested to ensure their qualification for seismic Category I service. The installation will meet quality assured Category I requirement. The staff finds this modification acceptable.

4.7.3.7 Class 1E Electrical Distribution System Changes From Temporary Modes of Manual and Automatic Operation to the Final Design Configuration

(1) Pending qualification of the new TDI EDGs, certain manual and automatic means of operation were proposed by the licensee and approved by the staff in Amendment 68. These operations were necessary to provide emergency ac power to additional essential Class 1E equipment added and designed to be powered by the new EDGs, as shown on Figure 4.2 of this supplement. This was accomplished by automatic closure of train B load center tie breakers in the case of loss of offsite power to train B and consequent start of the associated EDG. By using the load center tie breakers, both 4160-V buses (S4B and S4B2) and both 480-V buses (S3B and S3B2) in train B can be supplied by the old EDG (Bruce GM-GEB). The load center tie breakers in train A were manually closed for the conditions and purpose, similar to those for train B. For the final configuration when the new TDI EDGs in both trains are in service, these tie breakers will only be used for maintenance during cold shutdown. The automatic closure circuitry of the B train load center tie breakers for the loss of offsite power (LOOP) will be removed. Both train load center tie breakers will be operated only manually. During normal operation, these breakers will be racked out and kept under administrative control. Additionally, interlocks will be provided between the tie breakers and the main feeder breakers to the load center buses such that each tie breaker can be closed only if at least the feeder breaker to one of the two load center buses is open. This feature will prevent paralleling of the two EDGs in a train. In the final configuration, the interdependence of the two 4160-V buses in both trains will be removed, thus increasing the train reliability. In the event of a LOOP to any one of the four 4160-V Class 1E buses, its associated undervoltage scheme will cause tripping of its offsite source feeder breaker, starting of the associated EDG, and initiation of the bus unloading (load shed) and loading (load sequencing) scheme, independent of the other EDG in the same train or the redundant train. The staff finds this change acceptable.

(2) During the interim period until the new TDI EDGs are placed in service, the automatic start of certain essential heating, ventilation, and air conditioning (HVAC) systems was blocked (staff review in Amendment 68) during LOOP conditions to provide the total capacity of the existing EDGs to only the safety loads. These blocking circuits will be removed before restart and the HVAC loads will be automatically loaded on to their respective EDGs. In addition to the blocking circuits, timers were provided to allow closing of the essential HVAC system feeder breakers during a LOOP or ESFAS with LOOP, following closure of the maintenance tie breakers. The proposed modification will remove the timers and replace them with electric reset relays to provide a maintained close permissive for the load sequencer to automatically close the HVAC system feeder breakers. The licensee's proposal also includes providing similar electric reset relays to provide a similar function to the load center bus supply circuit breakers. This modification eliminates dependence on the timer and allows the sequencer to close the breakers. The reset relays will be qualified to the requirements of IEEE Standard 323-1974 and IEEE Standard 344-1975. The staff finds this modification acceptable.

(3) The existing sequencer loading status indicating lights at the control room panel are located in the back panel and below the standing line of sight making it difficult to read. The proposed modification will remove these lights from the back panel and will relocate the sequencer loading status indication for all the four sequences at the computer (IDADS) in the control room. Indication via IDADS is better as it provides also a backup means of indication. Furthermore, an audible alarm will also be generated from the computer. The change does not involve device addition and equipment qualification. Isolation between the Class 1E control circuits and IDADS is evaluated in a separate staff review (part of the startup SER). The staff finds this modification acceptable.

(4) In the Rancho Seco design, the physical position of the battery charger output circuit breaker is not monitored as required by Section 5.3.4(5)c of IEEE Standard 308-1974. Instead, the charger failure alarm and administrative control was used for this function. A confirmatory item of Amendment 68 required the licensee to install "battery bank voltage monitoring" to reflect the charger output breaker open or close positions. The proposed modification is to install undervoltage relays to monitor voltage on the 125-V dc Class 1E buses. The relays are set at 125 V with a 30-second time delay alarm via the IDADS. Since the battery is floated at 130 V dc, a drop to 125 V will indicate loss of input from the battery charger and thus the position of the battery charger output circuit breaker. The proposed 30-second time delay will prevent undesirable alarm due to transients. The relays are qualified to the requirements of IEEE Standard 323-1974 and IEEE Standard 344-1975 and will be installed to quality assured Category I requirements, maintaining the seismic qualification of the dc panels. The staff finds this modification acceptable.

(5) During the interim period until the new TDI EDGs are placed in service, the Rancho Seco design provided interlocks to prevent the pressurizer heaters from being energized by the existing EDGs if the reactor building spray pump is energized. The purpose of the interlock was to prevent overloading the existing EDGs beyond their capacity and to use the available capacity of the EDGs for only the safety loads. The proposed modification eliminates these interlocks and permits the pressurizer heater energization from the new TDI EDGs on demand. There will no longer be a need to block the energization of these heaters when the new EDGs are put in service. The staff agrees with the licensee's approach and finds the modification acceptable.

4.7.3.8 Conclusions, Class 1E Electrical Distribution Systems Associated With the Diesel Generators

The staff has reviewed the Class 1E electrical distribution systems, including the design modifications that had not already been reviewed in NUREG-1286, and finds them acceptable. The issue of Class 1E electrical distribution systems associated with the diesel generators is closed as a restart item.

4.7.4 Diesel Generator Fire Protection Considerations

In the SER related to the restart of Rancho Seco (NUREG-1286), the staff reviewed the diesel generator fire protection considerations, and concluded that the design

of the TDI diesels, DG building, and supporting systems conforms with BTP CMEB 9.5-1 and Appendix R to 10 CFR 50 and is, therefore, acceptable.

4.7.5 TDI Diesel Generator Building Design

4.7.5.1 Seismic Design of Diesel Generator Building

The design criteria provided by the licensee are identified in its Updated Safety Analysis Report (USAR), Volume III, Section 5.1 ("Structures and Containment System") and Section 5.3 ("Auxiliary Building"), dated July 1982; and in its Design Basis Report ECN A-3748, Revision 7, December 1, 1986; these reports describe the design criteria used in the analysis, design, and construction of the diesel generator building (DGB). The staff reviewed these criteria and found them consistent with those of the original Final Safety Analysis Report (FSAR) submitted in 1971 and approved by the staff on June 8, 1973.

The key structural design criteria used in the design of the DGB include: (1) the safe shutdown earthquake (SSE, originally designated as design-basis earthquake, DBE, in the FSAR) is 0.25 g and operating-basis earthquake (OBE) is 0.13 g; (2) free-field design spectra are in accordance with the provisions of RG 1.60; (3) design time histories are developed in accordance with the previously approved methodology; (4) the modeling techniques and analytical procedures for seismic analysis of the building were also found consistent with the acceptable procedures, and (5) the damping values and the lumped parameter representation of the building and the combination of spatial components of earthquake forces used in the analysis are acceptable. The concrete structural elements are designed in accordance with American Concrete Institute (ACI) Specification 349-80, subject to additional provisions described in RG 1.142.

The appropriateness of the licensee's use of the 15% damping value in its cable tray design is acceptable in that the cable tray systems used in the building are similar to those used in the damping test program referred to by the licensee in support of the 15% value.

On the basis of the results of its review and plant site audit, the staff concludes that the proposed diesel generator building conforms to applicable FSAR seismic design criteria and requirements, and is acceptable for plant restart.

4.7.5.2 Tornado Design of Diesel Generator Building

The staff has evaluated the capabilities of TDI diesel generators and their ancillary components to withstand the effects of high winds, including tornadoes. With three exceptions, all structures and components associated with the diesel generators are protected against the effects of the facility design-basis tornado of 175 mph and the missiles associated with these winds.

The three items not adequately protected are:

(1) the radiators
(2) oil storage tank vent lines
(3) day tank vent lines

The Rancho Seco diesel generator radiators are not protected from airborne tornado missiles that could over-top the radiator exterior walls. To address this issue, the licensee has performed a probabilistic risk assessment (PRA) of the likelihood of this occurrence. The licensee estimates that the probability of the over-topping tornado missiles damaging the radiators is approximately 5.6×10^{-8}/per year. The staff had questions about various assumptions used by the licensee in its assessment but agrees that the probability of occurrence of such an event is quite small. Because this event is extremely unlikely to occur, the staff and licensee have agreed that either the staff's concerns with regard to these PRA assumptions will be resolved or that the licensee will protect the radiators from airborne tornado missiles during the next refueling outage after plant restart.

Regarding the exposure of fuel oil storage tank fill and vent lines to damage from tornado missiles, the tanks themselves are located underground and are protected from effects of tornadoes and tornado missiles. The storage tank fill and vent lines, however, are located above grade without any tornado missile protection. It is possible for a tornado missile to render the fill and vent lines inoperable. Should this happen, an alternate means of resupplying the storage tank through the grade level manhole is available. The manhole is readily accessible. Should the vent line be damaged, the storage tank can also be vented through the manhole, or via the fuel oil day tank through the day tank overflow.

The staff concludes that the probability of tornadoes or tornado missiles rendering the TDI diesel generators or any of the critical structures or components for these diesel generators inoperable is acceptably low.

4.7.5.3 Ventilation, Communication, and Lighting Design of Diesel Generator Building

Ventilation Systems

The two emergency diesel generators (EDGs) that are the subject of this evaluation are completely independent of each other. Each is located in a separate room within the EDG building, and there is a ventilation system for each diesel generator. There is a separate control room with a ventilation system for each diesel generator, and the electrical distribution equipment for each diesel generator is located in a separate part of the nuclear service electric building (NSEB). Each part of the NSEB has its own essential HVAC system. There are no shared ventilation systems between diesel generators, nor are there any electrical interconnections. This conforms to GDC 5 with regard to shared systems, and GDC 17 with respect to electrical independence. All ventilation systems described above are under all design-basis conditions. This conforms to GDC 2 with respect to seismic qualification, and to GDC 4 with respect to maintaining design limits. Any single failure in any ventilation system will not result in the loss of more than one diesel generator. All ventilation system components associated with the diesel generators are housed in Category I structures that are above the maximum flood level and provide protection from tornadoes and tornado missiles. Any internally generated missiles would be contained within a diesel generator system and would not impact the other diesel generator and its related components. There are no high-energy lines associated with the diesel generators. All nonessential components are seismic Category II; i.e., they will not fail impairing operation of essential components.

On the basis of its review of the data and other information provided by the licensee, the staff concludes that the design of the engineered safety features ventilation system (ESFVS) meets the Commission's regulations as set forth in GDC 2, 4, 5, and 17 and are acceptable.

The licensee's design of the ventilation systems for the battery rooms within the NSEB were evaluated as part of the review conducted for the change implemented in Amendment 68 to the Rancho Seco operating license. These ventilation systems were found acceptable at that time.

Communication Systems

The scope of this evaluation is limited to the communication capability between the existing control room and the new EDG building and the NSEB. Intraplant and plant-to-offsite communications, including paging and alarm systems, are part of the original plant design and are not reconsidered here.

The EDG building will be included in the plant paging system, and flashing amber lights will be provided in high noise areas to augment the audible evacuation signal. The licensee's submittal did not make any reference to voice communications between the DG building and the control room. In response to specific staff questions regarding communications, the licensee stated that seismically mounted sound-powered phones would be installed in the DG control and engine rooms. The sound-powered phones would provide communication with the control room.

Sound-powered phones are essentially passive components; i.e., they do not require a dedicated ac or dc power source such as is required by a paging system or conventional telephone system, nor do they require an antenna or repeater in order to function. Therefore, a seismically mounted, sound-powered phone system can be relied on for communication during and after any design-basis event. On this basis, the staff concludes that the licensee's communication systems for the EDG building and the NSEB are acceptable.

Lighting Systems

The scope of this evaluation is limited to the lighting systems in the EDG building and the NSEB. Lighting in other plant areas is part of the original plant design and is not reconsidered here.

During normal operation, lighting in the EDG building is powered from a non-Class 1 ac source and will provide illumination levels of about 30 footcandles. The lighting fixtures are seismically supported, but the power to the lights is not Class 1E. The lighting transformers and distribution panels are not seismically qualified, and credit can not be given for their continued operation following a seismic event. Under these conditions, there would be no lighting in the EDG building following a seismic event. The staff has discussed this concern with the licensee. The licensee has indicated that battery-powered lighting capable of providing illumination for 8 hours will be installed in the EDG building. The battery-powered lighting would activate on a loss of ac power to the normal lighting system.

The staff finds the licensee's proposal acceptable for the following reasons. First, the battery-powered lights to be provided are seismically supported and can be relied on to function after a seismic event. Although the battery-powered lights will only function for 8 hours, and the need for lighting could greatly exceed 8 hours, the licensee has stated that the battery-powered lighting will be provided at the diesel generator control boards and will be manually switched on and off. With this arrangement, the lighting at the control boards would be used only when required as opposed to being continuously on, and would therefore be available intermittently for well in excess of 8 hours. The staff finds acceptable the concept of manually controlled, battery-powered, emergency lighting at the diesel generator control boards.

The basis for acceptance in the staff review was conformance of the design of the lighting systems and necessary auxiliary supporting systems to the acceptance criteria and guidance of SRP Section 9.5.3. Other bases for acceptance were conformance to industry standards, to NUREG-0700, and the ability to provide effective lighting in all conditions of operations.

On the basis of its review, the staff concludes that the lighting systems provided at Rancho Seco are in conformance with the above-cited standards and criteria, they can perform their design function, and are acceptable.

4.8 Cable Discrepancies

This section documents the staff's evaluation of the licensee's resolution of all remaining open items regarding deficiencies in design and installation of safety-related electrical cable. The scope of this issue and the licensee's program addressing it are described in detail in Section 4.8 of the restart SER (NUREG-1286) and are summarized below in Section 4.8.2.

4.8.1 Cable Discrepancy Background

In the years 1983 through 1985, the licensee undertook and completed a significant design/construction effort regarding electrical cable. These efforts involved redesignating the service level for existing raceway, rerouting existing cable, and installating new cable. This work was done in support of an expanded electrical distribution system, implementation of modifications for fire protection (Appendix R), and efforts to environmentally qualify safety-related electrical equipment. In the period, approximately 7800 cables were either installed or rerouted, including 2034 which had been designated as Class 1E. When compared with the design and installation of 14,000 cables in the original Rancho Seco plant, the licensee's effort was clearly an ambitious one.

Cable problems began to surface in 1984 when it was alleged that records documenting electrical cable installation were missing and were not properly controlled, and that data entered into the computerized cable and raceway tracking system (CRTS) may be inaccurate. Subsequent investigation has substantiated these allegations. In 1985 and 1986, cable routing errors were discovered (LERs 85-16 and 86-10). Investigation of these incidents lead to the discovery of additional design and installation problems (LERs 87-13, 87-16, 87-24, and 87-26).

After discovering and investigating the misrouted cables, the licensee developed a plan for a limited amount of cable inspection. This plan was discussed with the staff in late 1986. In January 1987, all ongoing activities addressing cable-related problems were integrated into a single program under a single program manager.

4.8.2 Evaluation of Cable Discrepancies

Cable Discrepancies Action Plan

The licensee's program for resolving cable problems has consisted of five principal activities: (1) formal investigation and root cause evaluations, (2) inspection of installed cable, (3) analysis of CRTS data to identify cable raceway design and installation deficiencies, (4) engineering evaluation and disposition of identified deficiencies, and (5) implementation of corrective actions. All program items regarding safety-related cable and raceway have been completed.

However, some actions regarding non-Class 1 cable and raceway will be completed before restart following the cycle 8 refueling outage. Completed items and open items are listed in Attachment 1 to the licensee's Wire and Cable Program Report (letter of December 4, 1987).

The staff's evaluation of the licensee's program is based on the review of formal submittals (licensee's letters dated April 3, July 21, August 18, October 12, November 9, December 4, and December 17, 1987). The staff has reviewed the licensee's root cause evaluation of design and installation problems, scope and completeness of the inspection program, engineering evaluation of identified problems, modifications to installed safety-related cable and raceway, and adequacy of corrective actions regarding programmatic deficiencies. Each of these areas is discussed below.

4.8.2.1 Evaluation of Root Cause of Cable Discrepancies

The licensee's Incident Investigation/Review Group (IIRG) has completed its review and investigation into the significant cable design and installation deficiencies and established root causes. The results of the investigations are documented in detailed investigation reports which have been provided to the staff (letter of December 17, 1987). Summaries of the root causes have been submitted separately (letter of November 9, 1987). Significant results of the investigations are summarized below, followed by the staff's evaluation.

Redundant Cabling in the Same Fire Area (LERs 86-10 and 87-13)

The cable routing discrepancies described in LERs 86-10 and 87-13 resulted when a field engineer failed to implement revisions to routing which had been directed and documented by design engineers. These failures took place during the 1984/85 outage. The route changes were part of a design change necessary in order to satisfy 10 CFR Part 50 Appendix R separation criteria for instrument cables feeding the control room and remote shutdown panel.

Cables were not rerouted primarily because the field engineer and construction card control group (CCG) engineering aide did not follow the established procedure for controlling cable installation records (i.e., procedure EII No. EC-10).

The investigation report indicates that the CCG engineering aide was poorly trained and was not even aware that the procedure existed. Consequently, installation records were processed in accordance with a procedure developed by the engineering aide. Under this procedure, cable pull cards were held by the CCG until the field engineer requested them, rather than transmitting them to the field engineer after receiving them from the cable and raceway tracking system. In addition, the engineering aide's procedure allowed the field engineer to hold the cards, as opposed to procedure EC-10 which required the field engineer to return the pull cards to the CCG upon completion of the work. These practices contributed significantly to the failure of the Nuclear Power Services (NPS) foreman (cable puller) to ever receive the cable pull order (i.e., card revision "c") to reroute the cables per Appendix R separation criteria.

Poor procedures and practices in quality control allowed the failure to reroute cables to go undetected. Existing quality control (QC) procedures called for in-progress inspection of cable installation including route verification. However, it was common practice for electrical QC inspectors to "inspect" cable pulls after they were completed and check routing as far as physically possible or by verifying terminations. One important factor that contributed to this practice was that cable installation quality records (i.e., the pull cards) were being held by field engineers until after the cable termination was made and then sent back to the CCG for transmittal to the electrical QC inspectors. Consequently, the CCG was notifying the QC inspectors to inspect pulled cable after the pull was completed.

Intermixing of Class 1E Power, Control, and Instrumentation Cable in the Same Raceway Contrary to Commitments in the USAR*

In one case, 3 power and 12 control cables were found intermixed with 36 instrumentation cables. This was the result of a failure to remove and reroute the power and control cables from their tray when the tray was redesignated as an instrument tray. Instrument cables were added to the newly designated tray as part of the same modification, which took place in the 1983 outage. The results of the investigation indicate that the power and control cables were pulled back per the work order, but then mistakenly repulled into their original trays rather than into power/control trays as intended. The investigator inspected the cable pull cards for the cables and noted that (1) the marking of the cards for cable rerouting was inconsistent and would be hard for both field installation and QC personnel to follow and (2) the pull cards were signed by the field engineer rather than by the foreman responsible for pulling the cable as required by procedure EC-10.

During the licensee's review of the CRTS database, one power cable and one control cable were found routed in an instrumentation cable tray. The cause of this discrepancy has been determined to be a design error: The instrumentation tray had originally been a power/control tray that contained the two power and control cables and those cables were not specified for removal and rerouting, as they should have been, when the tray designation was changed from power/control to instrumentation as part of electrical modifications in 1983.

---

*USAR: "Rancho Seco Nuclear Generating Station Updated Safety Analysis Report."

During its review of the CRTS database, the licensee identified 15 power and 7 control cables routed in instrument trays and 6 instrumentation cables routed in power and control trays. The investigation revealed that these cables had all been misrouted during the original design and construction of the plant and were most likely the result of isolated design errors. However it was also discovered that some of these cables had been rerouted since the beginning of commercial operation and were rerouted again in trays of a different service level. The root cause of the original design errors is not clear. The root cause of the rerouting errors appears to be that the physical layout designers who rerouted the cable were unaware of the USAR requirement that instrumentation cables not be mixed with power and control cables. A contributing factor was that the CRTS did not track service level explicitly and consequently did not include a check for mixing.

Overweight Cable Trays

On February 25, 1987, it was determined that up to seven cable trays might have exceeded the 50 pounds per linear foot limit of the USAR. These potential overweight cable trays were reported in LER 87-24, Rev. 0. Later evaluation revealed that one tray exceeded the weight limit by a small and acceptable amount (about one pound).

The investigation revealed that ever since the plant was designed, cable tray fill limits were treated as guidelines that could be exceeded as long as weight limitations were not exceeded; and, that the weight checks were done informally and not documented. It also found that while procedures specified fill limits, they did not address the basis for the limit nor the conditions under which it was acceptable to exceed the limit. Also, in 1985, a design procedure for the cable system was modified to increase the fill limit for instrumentation trays from 40% to 50%. However the 40% limit in the USAR was not revised.

The investigators concluded that the direct cause of the overweight cable tray problem was inadequate procedural guidance; the root cause was failure to ensure adequate implementation of USAR requirements.

Pulled Cables Stored in Safety-Related Breaker Cubicles

On February 5, 1987, electrical maintenance workers determined that lock-out relays in two safety-related cabinets could be inadvertently actuated if touched by cables coiled in the same cabinet. Actuation of the lockout relays in two of the cabinets would result in loss of normal and emergency power to a safety bus. On February 6, 1987, it was determined that the presence of these coiled cables invalidated the seismic analysis for the cabinets. Later, all the safety-related cabinets were checked and cables were found coiled in four other cabinets.

The investigation of this event included a detailed review of applicable cable installation procedures and revealed the following significant deficiencies:

(1) Existing procedures allowed cable to be pulled and coiled into a cabinet with termination at a later date, but did not include guidance as to what types of equipment could have cables stored in them until termination or when seismic qualification of equipment is invalidated by the presence of spare coiled cable.

(2) Coordination between groups responsible for pulling and terminating cable was not addressed in procedures as it should have been.

The root cause of cables being left coiled and unrestrained in safety-related breaker cubicle cabinets was determined to be inadequate procedures for the installation of electrical cables.

Cable Raceway and Tracking System Discrepancies

The CRTS consists of a computerized database and a set of algorithms used to store, retrieve, and analyze design and installation information regarding electric cable and raceways in Rancho Seco. It was developed by the licensee in the late 1970s and early 1980s to support a significant number of electrical system modifications being planned, improve cable/raceway design capabilities, and reduce the overall cost of tracking cable and raceway. Part of the development included loading data from the system used during original plant construction into the new system and making it compatible with the software in the CRTS.

The development and application of the CRTS were investigated after:

(1) allegations that the system was not used correctly and that errors were being entered into the database

(2) indications that the CRTS database did not match the actual plant configuration (LERs 86-10, 87-13)

(3) questions raised by NRC inspectors about the quality of the CRTS database

The investigation report indicates that the accuracy and overall quality of the CRTS has suffered from lack of proper quality assurance (QA) during development, extreme difficulty in making the original tracking system data compatible with the CRTS, and lack of procedures for entering and controlling data in the CRTS. Preoccupation with these problems appears to be one reason that the CRTS was ineffective in flagging cable design and installation problems. The root cause of CRTS problems is identified as a lack of proper management oversight in the development and use of the system.

Staff Evaluation

The staff has reviewed the investigation reports provided by the licensee (letter of December 17, 1987) and discussed the results with individual investigators. On the basis of the investigators' review, the staff believes that the investigation of cable problems has been of sufficient scope and depth to determine root causes and yield meaningful recommendations. The recommendations that have come out of the investigations have been formally reviewed and dispositioned as part of the licensee's corrective actions program. The results are discussed in Section 4.8.2.4.

Considering its review of the investigation reports and the documented level of control exercised by the licensee in installing cable between 1975 and 1986, the staff has concluded that several significant deficiencies led to the errors in electrical system design and construction. They include:

(1) lack of adequate procedures for the construction and QA of electrical cable installations

(2) poor practices in the design, construction, and QA of electrical cable installations, and the apparent acceptance of those practices by supervisors

(3) inadequate staffing and training in field engineering and quality control (QC) activities

(4) poor supervision in field engineering, QC, and CRTS activities

(5) lack of effective communication between electrical design engineers and regulatory compliance engineers

4.8.2.2 Cable Inspection Program

The scope of the Cable Discrepancies Action Plan included 2034 safety-related and safe-shutdown cables that were installed or rerouted since start of commercial operation of the Rancho Seco power plant.

The licensee's program for inspecting cable routes and the staff's evaluation of that program are documented in the original Rancho Seco Restart SER (NUREG-1286). Basically, the licensee's action plan program consists of a complete (100%) inspection of all safety-related and safe-shutdown cables that have involved route revisions between the start of commercial operation and the initiation of the inspection program (cable lots 1 and 4); and a random sample inspection of cables installed between the beginning of commercial operation and the initiation of the inspection program; and, cables that have never undergone route revisions (cable lots 2 and 3). The staff has accepted the difference in emphasis regarding the two "types" of cable based on the results of the root cause investigations of cable discrepancies. As discussed in Section 4.8.2.1, the fundamental breakdowns in the control of cable installation significantly increased the likelihood that routes would not be revised and that those errors of omission would go undetected. Results of both the root cause evaluations and inspections clearly indicate that incompetence on the part of installers during cable pulling operations was not the problem. The staff considers it much less likely for implementation errors in new, non-revised cable installations to occur or to go undetected, since the weakness in controls occurred in the way changes were processed; and, inspection of cable terminations and post-installation testing of associated equipment would normally detect a failure of a field engineer to implement a work request to install a new cable.

Results of Inspections

The licensee completed the cable inspections in late October 1987 and documented the results in its Wire and Cable Program Report enclosed with the licensee's letter of December 4, 1987. However, later review of cable records indicated that three cables from lot 2 did not truly satisfy the definition of the lot 2 cable population, making it necessary to complete three additional cable inspections. These inspections were completed on December 9, 1987 and the results were documented in the Wire and Cable Program Report enclosed with the licensee's letter dated January 22, 1988.

Table 4.6 summarizes the results of all inspections. The number of major and minor defects in cable routing are listed for each cable lot along with population size and sample size. Recall that lots 1 and 4 include rerouted cables and lots 2 and 3 include cables that have never been rerouted. A major defect is defined as a cable route that differs from the cable and raceway tracking

Table 4.6 Results of cable inspections

Description	Lot 1	Lot 2	Lot 3	Lot 4
Population size	397	1383	176	78
Sample size	397	91	51	78
Cables inspected	397	91	51	78
Major defects	12	0	0	7
Minor defects	38	4	1	2
Insignificant or no defects	347	87	50	69

system (CRTS) recorded route and the difference constitutes a violation of the NRC requirements or plant design criteria. A minor discrepancy is defined as a routing that may vary from that listed by the CRTS, yet is acceptable from a safety and design standpoint. An insignificant defect is a cable route that differs from the CRTS recorded route only to the extent that typographical errors exist in the recorded data. As indicated in Table 4.6, nineteen major defects were identified in a 100% inspection of rerouted cables and no major defects were found in the inspection of a 9.1% sample of cables that have not been rerouted.

The lot 2 and 3 sampling task was a "hypotheses testing" of a finite population to achieve a 95/95 assurance, i.e., 95% assurance that at least 95% of the cables of lots 2 and 3 are correctly routed. The confidence level established by the 95/95 acceptance criterion is the conditional probability that the percentage of major defects in the total population is less than or equal to five. The staff has accepted this approach when it is determined that the defects have no significant potential for a loss of redundancy due to a single failure during a design-basis accident. The types of major defects identified at Rancho Seco that could impact plant safety are:

(A) Redundant safety cables in the same fire area where a single fire could cause a loss of redundancy.

(B) Lack of acceptable separation between Class 1E and non-Class 1E cables. In this case a sustained, uninterrupted overcurrent in the non-Class 1E cable could impact the unseparated Class 1E cable resulting in a loss of safety function.

(C) Lack of acceptable separation between Class 1E instrument and power/control cables where a transient in a power cable could cause a spurious signal in the unseparated instrument cable.

However, for a single incident or accident to cause a loss of redundancy, the following must occur for the respective major defects:

Major Defect A

(1) Redundant safety cables must exist in the same fire area.

(2) A fire must be initiated.

(3) The fire detection/prevention system must fail.

(4) The fire must cause a loss of safety function in both IEEE Standard 383 qualified (fire retardant) cables.

(5) Neither loss of safety function is to a "fail-safe" condition.

Major Defect B

(1) A lack of acceptable separation must exist between a Class 1E and a non-Class 1E cable.

(2) A fault must occur in the non-Class 1E/circuit conductor or component.

(3) A failure must occur in the non-Class 1E circuit protective device failing to interrupt the fault.

(4) The effects of the fault in the non-Class 1E circuit must be sufficiently severe to adversely affect an adjacent Class 1E cable.

(5) The affected Class 1E cable does not cause a "fail-safe" condition.

(6) A simultaneous failure must occur in a redundant Class 1E circuit.

Major Defect C

(1) A lack of separation must exist between a Class 1E instrument cable and a power or control cable.

(2) An electrical transient must occur in the power or control cable causing a "spike" (electromagnetic induction) in the instrument cable.

(3) The magnitude of the induced "spike" in the Class 1E instrument cable must be sufficient to initiate a spurious action or indication in the instrument circuit.

(4) A simultaneous failure must occur in a redundant instrument circuit.

The licensee has maintained that there is a remote likelihood of simultaneous occurrence of the above-specified conditions which could cause concurrent or consequential failure of the redundant safety system. The licensee has identified earlier staff acceptance of 95/95 assurance level at other nuclear power plants for welds and concrete expansion bolts sampled to the same level.

Staff Evaluation

The staff has reviewed the results of the licensee's inspection program and confirmed that the results satisfy the commitments made previously by the

licensee and accepted by the staff. Considering the results of the inspections and the nature of the cable installation errors (see Section 4.8.2.1), the staff has concluded that the likelihood of installed safety-related and safe-shutdown cables being in a configuration that violates physical separation criteria is acceptably low. The staff also concludes that a potential for the redundant safety system failure due to a possible major defect (violation of physical separation criteria) is sufficiently low and is, therefore, acceptable.

With regard to the original cable population, the staff concludes that Bechtel quality control and Bechtel's circuit and raceway scheduling program provide sufficient assurance that the original cable design and installation were adequately controlled and thus had an insignificant potential for allowing a major defect.

4.8.2.3 Evaluation and Disposition of Cable Deficiencies

Each Class 1E cable deficiency identified in nonconformance or occurrence description reports has been evaluated insofar as its engineering and has been dispositioned. Deficiencies identified through analysis of the CRTS database, as well as walkdown inspections, are included. The problems that have been identified and addressed include: installed cable routes different from those in CRTS, intermixing of Class 1E cables with non-Class 1E cables; intermixing of power, control, and instrumentation cables; overfilled and overweight cable trays; overfilled conduits; accuracy of CRTS for raceway connections; documentation discrepancies; and missing or unsigned cable pull and termination cards.

The licensee has completed evaluation and disposition of all identified Class 1E cable discrepancies. All but one of the required physical plant modifications have been completed. The one remaining item involves replacement of a wire marker and is not considered significant by the staff.

The licensee has documented each individual discrepancy with its disposition in Attachment 2 of the Wire and Cable Program Report included with its letters of December 4, 1987 and January 22, 1988. The basis for each disposition is provided in Attachment 4 to the Wire and Cable Program Report. The staff has reviewed the dispositions and their bases against applicable NRC requirements and design criteria and found them acceptable. In performing its safety review, the staff has focused on the discrepancies involving misrouted cables, intermixing of Class 1E power and control cables with Class 1E instrumentation cables, and overfilled/overweight cable trays. Resolution of these issues is discussed below.

Misrouted Cable

Cables that have been misrouted to the extent that design criteria for physical separation were violated have been rerouted so that they now meet criteria. In addition, CRTS data have been corrected as necessary. Cables routed in conformance with all design criteria yet different from the route documented in CRTS were left in their as-found configuration. However, the CRTS was corrected to reflect the as-built configuration. The staff accepts this disposition because it ensures that installed cable meets design criteria and makes records consistent with the installed configuration.

Intermixing of Class 1E Cable

Of the 51 intermixed Class 1E cables, 35 were rerouted in a raceway of the appropriate service level. The 14 low-energy power cables originally routed with associated instrumentation cables for reactor coolant system (RCS) flow transmitters have not been rerouted. The licensee considers this disposition acceptable for the following reasons:

(1) The power and instrument cables function together to operate RCS flow transmitters. They are part of the same flow transmitter circuitry. The manufacturer's intent was clearly to run both cables in the same raceway.

(2) Each power cable and its associated instrument cable share a dedicated conduit for about 120 feet within the reactor building, since the transmitter has only one conduit entry.

(3) Because the power requirement of the transmitter is low, the current is small (70 mA) and, consequently, the magnetic field produced by it is small.

(4) Twisted shielded pair cable is used for both power and signal cables. This minimizes the effects of electromagnetic and electrostatic noise.

(5) There have been no recorded fault or spurious signals caused by the flow transmitters during plant operation with the cables as mixed in 1985.

The staff accepts the licensee's disposition regarding the cabling of the RCS flow transmitters since it is based on sound engineering judgment and operating experience.

The two other intermixed Class 1 cables are instrument cables routed in power and control raceway. The cables provide tachometer indication signals to local panels of the Bruce GM diesel generators. The cables have not been rerouted because they affect only an indicator and not any safety function of the diesel. The staff accepts the licensee's disposition based on the relative safety significance of the cables in question.

Overweight and Overfilled Class 1E Cable Trays

The licensee has checked all instrument cable trays for weight with calculations based on CRTS data. No trays were found to exceed the USAR threshold limit of 50 pounds per linear foot (lb/ft).

The licensee has checked all power and control trays for weight, regardless of fill level. No Class 1E trays exceeded the weight limit of 50 lb/linear foot. Ampacity checks were also performed on all power and control trays with fills in excess of 40%. No deficiencies were found.

The staff believes that the scope of the licensee's review of cable weight and fill concerns has been adequate.

4.8.2.4 Actions To Correct Cable Discrepancies

Hardware Modifications

All cable discrepancies needing physical plant modification for resolution are documented in Attachments 2 and 3 to the licensee's letter of December 4, 1987. The majority of the modifications have involved rerouting safety-related or safe-shutdown electrical cable to put it in conformance with design criteria. All necessary modifications involving Class 1E cable have been completed and their associated non-conformance reports have been closed (documented in letters of December 4, 1987 and January 22, 1988 and in telephone conferences held on December 11, 1987 and January 22, 1988).

Procedural Changes

In response to the cable design and installation deficiencies described previously (Section 4.8.2.1), the licensee has developed new procedures and controls and has also improved existing ones. The changes have been based on the results and recommendations that have followed from the root cause investigations. The licensee has provided an itemized description of the modifications to procedures and administrative controls that addresses each of the recommendations made by investigators (see items 29 and 30 in Attachment 4 to the licensee's letter of December 4, 1987). Some of the more significant changes are summarized below:

Redundant Cabling in the Same Fire Area (LERs 86-10,87-13)

A new procedure has been developed which establishes instructions for the processing of cable installation cards. The interfaces between the Card Control Group (CCG), CRTS Administrator, and Field Engineering are addressed. One important feature of the procedure is that it requires installation cards to be returned to the CRTS coordinator and held until the engineering change notice is closed. The procedure currently exists as an attachment to the nuclear engineering administrative procedure (NEAP) 4127, Revision 0, and is being formalized for future use as the Card Control Electrical Engineering Instruction. In addition, formal training on use of the procedure will be given to personnel who are either in the CCG or who handle cable installation cards in interfacing groups.

Existing cable installation procedures (MP/IS 307) have been revised so that cable route inspection is specified as a "hold point" in the procedure and QC inspectors are required to witness cable pulls. In addition, electrical QC inspectors have been trained in this procedural clarification.

Cable route revisions and repulls are to be specified explicitly on the cable drawings and forms input to the CRTS. Changes to these documents that result from route revisions will be treated as drawing change notices (DCNs). New installation documents will not be generated for repulls.

Design Control - Intermixing of Power, Control, and Instrumentation Cables

Electrical design guides have been revised to clearly specify design requirements for physical separation of power, control, and instrumentation cable in raceway and manholes, and to make them consistent with USAR requirements.

Cable service level (i.e., power, control, and instrumentation) have been included as inputs to CRTS.

Overweight Cable Trays (LER 87-24)

Cable tray weights have been calculated for all trays exceeding fill limits. One Class 2 tray which was slightly above the 50 lb/ft limit was modified to correct the problem. All other trays were found to be within the limit.

CRTS operating procedures (NEAP 4127) have been prepared that require input to be checked against fill criteria by CRTS personnel and rejected if limits are exceeded. Cable trays are then reanalyzed and those that cannot meet weight or ampacity limits are to be redesigned and resubmitted to CRTS.

Controls now require that design changes that cause tray weight to exceed a threshold of 50 lb/ft will not be accepted without a review against applicable design limits per 10 CFR 50.59.

Pulled Cables Stored in Safety-Related Breaker Cubicles (LER 87-16)

Cable installation procedure MP/IS 307 is being modified to address the root causes of cable storage problems.

Cable Raceway Tracking System

The procedure NEAP 4127, Revision 0, "Cable and Raceway Tracking System," was issued on June 15, 1987 and controls the method by which proposed changes to the CRTS data base are submitted, approved, and incorporated. Implementation of NEAP 4127 formally places the CRTS operation within the licensee's quality assurance program.

Procedure NEAP 4112 is being revised so that it applies to CRTS input documents and forms. NEAP 4112 covers preparation, processing, and incorporation of drawing changes. Treatment of CRTS input documents in this way will improve controls on implementation of cable route revisions. Modification of NEAP 4112 formalizes this process which has been in place since May 1, 1987.

Staff Evaluation

The staff has reviewed the corrective actions that have been implemented and finds them acceptable. The basis for acceptability is that the corrective actions specifically address root causes that have been identified through thorough investigation of individual cable discrepancies.

4.8.3 Conclusions, Cable Discrepancies

In regard to the cable issue, the staff concludes that because the licensee was ill equipped to undertake a major electrical design and construction effort, a number of errors in safety-related activities escaped the normal quality assurance reviews. However, after thorough investigation of the problems, the licensee developed and has implemented an acceptable corrective actions program. Defects in safety-related cable installations have been evaluated and corrected and necessary changes in procedures and controls have been adopted.

The staff finds that the programmatic changes will be effective in the future, provided they receive strong management support and are implemented with a commitment to quality.

The issue of cable discrepancies is closed as a restart issue.

4.9 Technical Specification Evaluation

Section 4.9 of the restart SER (NUREG-1286), issued in October 1987, presented in Table 4.4 a list of 27 risk-important systems and technical specification (TS) items, procedures, and improvements to be implemented before plant restart. These 27 items are listed in Table 4.7 of this SSER, with the resolution of each item.

In addition to proposing resolution of the 27 specific items identified by the staff in the SER, the licensee has proposed specific TS upgrade changes which have been evaluated and approved by the staff in Amendment 164. As a part of that overall upgrade, the licensee has proposed and the staff has approved a TS revision which adds the Standard Technical Specification (STS) General Limiting Conditions for Operation statements (STS 3.0.1 through 3.0.4) to the Rancho Seco Technical Specifications. The licensee also has committed to a complete upgrade of the Rancho Seco TS consistent with the new STS which are being developed by the B&W Owners Group. The licensee intends to implement the upgraded TS before startup after the first refueling outage following plant restart.

Since each item in Table 4.4 has been resolved in an acceptable manner, the licensee's response to NUREG-1286, Section 4.9, is acceptable, and this issue of Technical Specification evaluation is closed as a restart issue.

4.10 Other Issues Related to Rancho Seco Restart

Two other issues that developed during the latter stages of the staff's review are addressed below.

4.10.1 Operating Experience Feedback Report: New Plants (NUREG-1275)

By letter dated September 1, 1987, the licensee was sent a copy of NUREG-1275, "Operating Experience Feedback Report: New Plants," with a request to consider the "improvement lessons" contained in Section 5 of the report in the light of impending startup of Ranco Seco following a long outage. By letter dated January 19, 1988, the licensee submitted a report, "Rancho Seco Nuclear Generating Station Response to NUREG-1275," dated January 1988. The NRC staff has evaluated that report and, on February 16 and 17, 1988 the staff visited the site and met with the licensee to review the licensee's activities that are responsive to the improvement lessons contained in Section 5 of NUREG-1275.

The staff finds that the licensee has been responsive to concerns expressed in NUREG-1275 in its preparation for restart of Rancho Seco. The staff's evaluation of this issue is more completely set forth in the AEOD Special Report, "Operational Experience Feedback Evaluation, Rancho Seco Nuclear Generating Station, Restart," dated March 1988. The staff will follow up on recommendations contained in the evaluation regarding methods and procedure modification for post-event analyses, and adequacy of surveillance procedures and personnel training on these procedures. The staff finds the licensee's response to be appropriate for restart of the plant.

Table 4.7 Technical Specification/procedure/commitment improvements needed before restart of Rancho Seco (revised from SER Table 4.4)

Item*		Specification	Resolution
(1)	Provide action statement on steam generator operability.	STS 3.4.6**	Resolved in Amendment 152 and with the addition of Amendment 164.
(2)	Provide action statement on ECCS injection system operability.	STS 3.5.2	Resolved in Amendment 164 with the addition of Sections 3.0.3 and 3.0.4.
(3)	Provide action statement on ECCS core flooding system.	STS 3.5.1	Resolved with addition of action statement in RSTS 3.3.1 *** in Amendment 164.
(4)	Provide action statement on ECCS reactor building spray.	STS 3.6.2.2	Resolved with addition of action statement in RSTS 3.3.1 in Amendment 164.
(5)	Provide action statement on ECCS allowed outage time.	RSTS 3.3.2	Resolved with addition of Sections 3.0.3 and 3.0.4 in Amendment 164.
(6)	Provide commitment for operability of ac onsite power distribution.	STS 3.8.2	Resolved in Amendment 147 and with action statements contained in Amendment 164.
(7)	Provide action and surveillance statements on reactor building penetrations during refueling.	STS 3.9.4	Resolved via implementation of RSTS 3.8.9 and the addition of Section 3.0.4 in Amendment 164.
(8)	Add requirement for rod/channel position indication operating.	STS 3.1.3.3	Resolved with the information found in RSTS Table 4.1-2 and 4.7.1. In addition Sections 3.0.3 and 3.0.4 of Amendment 164 are acceptable.
(9)	Add limiting condition for operation for unacceptable rod-drop time.	STS 3.1.3.5	Resolved with information found in RSTS 3.5.2.2.

*As listed in NUREG-1286 (Rancho Seco Restart SER).
**STS = NUREG-0103, Rev. 4, "Standard Technical Specifications for Babcock and Wilcox Pressurized Water Reactors," September 1980.
***RSTS = "Technical Specifications for the Rancho Seco Unit 1" (based on numbering scheme in use February 1987).

Table 4.7 (Continued)

Item*	Specification	Resolution
(10) Add rod program requirement.	STS 3.1.3.5	Resolved with information found in RSTS 4.7.2.3 and 1.3 "operable."
(11) Add requirement on nuclear heat flux-hot channel factor.	STS 3.2.2	Resolved with information found in RSTS 2.1.
(12) Add requirement on nuclear enthalpy rise-hot channel factor	STS 3.2.3	Resolved with information found in RSTS 2.1.
(13) Add commitment on remote shutdown instrumentation.	STS 3.3.3.5	Resolved with addition of Items 84-90 of RSTS Table 4.1-1 in Amendment 164.
(14) Provide commitment on ECCS operability for operation/hot and cold	STS 3.5.3	Resolved with addition of Sections 3.0.3 and 3.0.4 in Amendment 164.
(15) Provide commitment for overall integrated containment leakage.	STS 3.6.1.2	Resolved with approval of RSTS 3.1.6.1 in Amendment 164.
(16) Provide commitment for limiting condition for operation and action statements for containment air locks.	STS 3.6.1.3	Resolved with approval of RSTS 3.6.1 in Amendment 164.
(17) Provide limiting condition for operation and action statements on containment air temperature.	STS 3.6.1.6	Resolved with addition of Section 3.0.3 in Amendment 164.
(18) Provide action statement on containment structural integrity.	STS 3.6.1.7	Resolved with information found in RSTS 4.4.2, 1.3 "operable," and 3.6. In addition Section 3.0.3 added in Amendment 164.
(19) Provide requirement on operability of hydrogen anaylzers.	STS 3.6.5	Resolved with information found in RSTS Table 3.5.5-1 and addition of Section 3.0.3 in Amendment 164.

Table 4.7 (Continued)

Item*	Specification	Resolution
(20) Provide commitment on operability of electrical power systems during shutdown	STS 3.8.1.2	Resolved with approval of RSTS Section 3.1.1.5A in Amendment 164.
(21) Provide commitment on operability of dc distribution system during shutdown	STS 3.8.2	Resolved with information found in RSTS definition of "operable."
(22) Provide TS on fuel storage pool water	STS 3.9.11	Resolved with addition of RSTS 3.9.5 in Amendment 164.
(23) Provide commitments to action statement on operation at all levels for ECCS-reactor building emergency cooling.	STS 3.6.2.3	Resolved with addition of RSTS 3.3.1C in Amendment 164.
(24) Provide commitment on periodic check of isolation valves outside containment	STS 4.6.1.1	Resolved with addition of RSTS 4.4.1.2.3(f) in Amendment 164.
(25) Provide commitment on containment penetration conductor overcurrent protection device.	STS 3.8.4	Resolved with determination that RS does not contain such devices.
(26) Provide action statement for operation with inoperable control rods.	STS 3.1.3.1	Resolved with addition of RSTS 3.5.2.2 in Amendment 164.
(27) Provide action statements for reactor building integrity (subcritical)	STS 3.6.1.1	Resolved with addition of RSTS 3.6 action statement in Amendment 164.

4.10.2 Safety and Performance Improvement Program

In January 1986, the B&W Owners Group (BWOG) Executive and Steering Committees initiated an effort directed toward reducing plant trips and improving plant responses to trips at B&W nuclear unit plants. The impetus for this effort was the recent occurrence of complex transients at Davis-Besse and at Rancho Seco, and NRC actions following those occurrences. As an outcome of those efforts, the BWOG Safety and Performance Improvement Program (SPIP) was formed. This program, described in detail in the BAW-1919 report, recommended 207 specific actions to be considered for implementation by each BWOG participant. By letter dated December 1, 1987, the licensee, Sacramento Municipal Utility District (SMUD), provided to the NRC staff a program list of all 207 SPIP recommendations, and a description of the classification and disposition for Rancho Seco of each recommendation. Other information on the subject was later requested and was provided to clarify the basis for disposition of certain SPIP recommendations.

Evaluation

The NRC staff has reviewed the licensee program for disposition, actions either taken or planned, in response to the SPIP recommendations. The BWOG SPIP Program List for Rancho Seco provided to the staff by letter dated December 1, 1987 generally contained sufficient detail to establish the basis for the licensee's disposition of each of the items in the list. Of the 207 items listed as SPIP recommendations, some 70 are designated as "key" items. These are designated by the BWOG as being most important and beneficial from a safety and performance improvement perspective. According to the current BWOG SPIP Recommendation Tracking System (RTS), 58 of the 70 "key" recommendations had been selected by SMUD to be implemented at Rancho Seco. Of those not so selected, or selected for the Long Range Scope List (i.e., not implemented before restart), the staff has looked at the basis for such disposition by the licensee. It should be noted that not all SPIP recommendations, "key" or otherwise, are appropriate for every plant having a B&W nuclear steam supply system.

The staff has also reviewed the results of an audit performed by a BWOG SPIP audit team at Rancho Seco, December 8-10, 1987, and has received the licensee's comments in response to the audit report. In order to assess the completeness of the licensee's program for implementing the SPIP recommendations and gain some perspective on the program for Rancho Seco as compared to other BWOG SPIP participants, the NRC staff has reviewed the SPIP Recommendation Tracking List for all BWOG SPIP participants.

On the basis of all the foregoing information, the staff finds that the licensee's program for disposition and implementation of the SPIP recommendations represents an acceptable effort to benefit from the program's recommendations. A more detailed discussion of particular applications of SPIP recommendations for reducing trips and increasing safety at Rancho Seco is given in this supplement. Discussion of such applications is found particularly in Section 3.1.2.4, "Loss of Instrument Air"; Section 3.1.2.8, "Power Supply Monitor Design"; Section 3.1.2.9, "ICS/NNI System Maintenance, Surveillance, and Testing"; Section 3.1.2.10, "Operator Response Procedures"; and Section 3.1.2.11, "ICS/NNI System Interactions With Safety-Related Equipment."

Conclusion

On the basis of the foregoing considerations, the NRC staff finds that the licensee's program for disposition of the BWOG SPIP recommendations is acceptable for restart of Rancho Seco.

APPENDIX A

PRINCIPAL MEETINGS AND CORRESPONDENCE
RELATED TO THE RANCHO SECO OVERCOOLING EVENT OF
DECEMBER 26, 1985

August 6, 1987	SMUD forwards "Maintenance Administrative Procedures Manual," per NRC request of August 4, 1987 (letter from G. C. Andognini, SMUD, to G. Kalman, NRC).
August 8, 1987	SMUD forwards final task lists of accredited programs to support NRC upcoming restart and post-accreditation training review (letter from G. C. Andognini, SMUD, to G. Kalman, NRC).
August 14, 1987	NRC forwards request for additional information and related submittals not received for plant restart (letter from G. Kalman, NRC, to G. C. Andognini, SMUD).
August 18, 1987	SMUD forwards Revision 1 to "Wire and Cable Program Report," dated July 31, 1986 (letter from G. C. Andognini, SMUD, to F. J. Miraglia, NRC).
August 26, 1987	NRC requests written statement regarding corrective and preventive measures taken to ensure conformance of safety-related fastener materials (letter from D. M. Crutchfield, NRC, to G. C. Andognini, SMUD).
August 27, 1987	NRC forwards Amendment 85 to License DPR-54 and safety evaluation, revising Technical Specifications to include fire protection components in auxiliary, turbine, and service nuclear electrical buildings and clarifies requirements on fire barriers (letter from G. Kalman, NRC, to G. C. Andognini, SMUD).
September 1, 1986	NRC transmits NUREG-1275 for information and consideration (letter from E. Jordan, NRC, to G. C. Andognini, SMUD).
September 16, 1987	SMUD submits Revision 2 to proposed Amendment 138, revising Technical Specifications to reflect additional organizational changes due to need for additional management staffing for present outage and from expansion of long-term management function (application from G. C. Andognini, SMUD, to F. J. Miraglia, NRC).

September 16, 1987	SMUD requests relief from Technical Specification 3.1.1.5 regarding inoperability of decay heat removal (DHR) system and reactor coolant system (RCS) during special test procedure STP.961, "Loss of Offsite Power Test" (letter from G. C. Andognini, SMUD, to F. J. Miraglia, NRC).
September 23, 1987	Meeting in Bethesda between NRC staff and SMUD representatives on progress of plant restart program (meeting summary dated October 15, 1987).
September 25, 1987	SMUD requests additional 30 days to respond to D. M. Crutchfield's letter of August 26, 1987, regarding results of chemical analysis and material testing of safety-related fastener materials obtained during maintenance inspection (letter from G. C. Andognini, SMUD, to NRC).
October 7, 1987	NRC forwards Safety Evaluation Report (NUREG-1286) regarding restart following the December 26, 1985 event and requests response to request of August 14, 1987 for additional information to resolve restart issues (letter from D. M. Crutchfield, NRC, to G. C. Andognini, SMUD).
October 8, 1987	SMUD forwards supplemental emergency diesel generator information per NRC request (letter from K. A. Meyer, SMUD, to F. J. Miraglia, NRC).
October 12, 1987	SMUD forwards additional information regarding instrumentation and control system/non-nuclear instrumentation maintenance, surveillance, and test procedures (letter from J. F. Firlit, SMUD, to F. J. Miraglia, NRC).
October 12, 1987	SMUD forwards report, "Rereview of Plant Instrumentation and Control for IE Bulletin 79-27" and Revision 0 to Engineering Report ERPT-0229, "Report on Response to NRC IE Circular 79-02" (letter from J. F. Firlit, SMUD, to F. J. Miraglia, NRC).
October 12, 1987	SMUD forwards Revision 2 to "Wire and Cable Program Report," per meeting (letter from G. C. Andognini, SMUD, to F. J. Miraglia, NRC).
October 13, 1987	SMUD forwards updated list of items deferred until after restart (letter from G. C. Andognini, SMUD, to T. E. Murley, NRC).
October 20, 1987	SMUD forwards Revision 0 to "Radiological Environmental Monitoring Program Manual," for review in support evaluation of proposed Amendment 155 to License DPR-54 (letter from G. A. Coward, SMUD, to F. J. Miraglia, NRC).

October 21, 1987	SMUD forwards fourth set of six expanded augmented system review and test program inspection reports on listed systems (letter from G. A. Coward, SMUD, to F. J. Miraglia, NRC).
October 22, 1987	SMUD forwards Revision 1 to D-0050, "Engineering Action Plan" (letter from G. A. Coward, SMUD, to F. J. Miraglia, NRC).
October 26, 1987	NRC discusses status of review and lists additional information needed to determine whether facility liquid effluent system is adequate to support plant operations (letter from G. W. Knighton, NRC, to G. C. Andognini, SMUD).
October 26, 1987	SMUD forwards response to request of October 8, 1987 for clarification and information regarding emergency diesel generator review (letter from R. G. Croley, SMUD, to F. J. Miraglia, NRC).
October 30, 1987	NRC advises that no Technical Specification relief is necessary to conduct tests on new emergency diesel generators and associated electrical distribution system (letter from G. M. Holahan, NRC, to G. C. Andognini, SMUD).
October 30, 1987	SMUD forwards plant Offsite Dose Calculation Manual (ODCM) for review to support evaluation of proposed Amendment 155 (letter from G. C. Andognini, SMUD, to F. J. Miraglia, NRC).
October 30, 1987	SMUD forwards requested additional information on proposed Amendment 147 to License DPR-54 and plant electrical distribution system (letter from S. F. Firlit, SMUD, to F. J. Miraglia, NRC).
November 9, 1987	SMUD forwards summary of root cause investigations of cable issues per G. Kalman's letter to G. C. Andognini of August 14, 1987 (letter from R. G. Croley, SMUD, to F. J. Miraglia, NRC).
November 9, 1987	SMUD discusses safety parameter display system (SPDS) safety evaluation issues regarding protection, software validation, and verification and electrical isolation (letter from R. G. Croley, SMUD, to F. J. Miraglia, NRC).
November 9, 1987	SMUD confirms that 15% damping value used during design of cable tray supports in Transamerica Delaval, Inc. (TDI) diesel generator building (letter from R. G. Croley, SMUD, to F. J. Miraglia, NRC).

November 10, 1987	NRC forwards safety evaluation supporting plant electrical distribution system design (reference TDI diesel generators) (letter from G. W. Knighton, NRC, to G. C. Andognini, SMUD).
November 11, 1987	SMUD meeting with Commission to present restart program progress.
November 11, 1987	SMUD forwards Revision 1 to "Radiological Environmental Monitoring Program Manual," for review to support proposed Amendment 155 (letter from G. A. Coward, SMUD, to F. J. Miraglia, NRC).
November 12, 1987	SMUD forwards description of radioactive liquid effluent system (letter from G. C. Andognini, SMUD, to F. J. Miraglia, NRC).
November 13, 1987	SMUD discusses audit on restart and long-range scope list (RSL/LRSL) completed on November 12, 1987 (letter from G. C. Andognini, SMUD, to J. B. Martin, NRC).
November 20, 1987	SMUD forwards additional audit information regarding matrix of SPDS equipment versus qualification (letter from G. A. Coward, SMUD, to F. J. Miraglia, NRC).
December 1, 1987	SMUD transmits BWOG SPIP list for NRC information and use (letter from G. C. Andognini, SMUD, to G. Kalman, NRC).
December 4, 1987	NRC requests additional information regarding review of integrated control system (ICS) and non-nuclear instrumentation (NNI) system (letter from G. Kalman, NRC, to G. C. Andognini, SMUD).
December 4, 1987	SMUD forwards Revision 3 to "Wire and Cable Program Report" per commitment of May 6, 1987, (letter from G. C. Andognini, SMUD, to F. J. Miraglia, NRC).
December 7, 1987	NRC staff meets with SMUD at plant site regarding recent events at facility, control room heating, ventilation, and air conditioning (HVAC), and facility readiness for restart (meeting summary by L. Miller, Region V, dated December 14, 1987).
December 9, 1987	NRC forwards "Program for Evaluating Licensee Conformance to Revision 2 to Regulatory Guide 1.97 and SPDS Implementation," Site Audit Report of the October 26-28, 1987 audit (letter from G. Kalman, NRC, to G. C. Andognini, SMUD).
December 12, 1987	SMUD forwards additional information on plant SPDS (letter from G. A. Coward, SMUD, to F. J. Miraglia, NRC).

December 14, 1987	NRC advises of NRC concern regarding licensee failure to provide restart prerequisite submittals as scheduled (letter from G. Kalman, NRC, to G. C. Andognini, SMUD).
December 14, 1987	NRC forwards safety evaluation accepting emergency feedwater initiation and control system design (letter from G. W. Knighton, NRC, to G. C. Andognini, SMUD).
December 15, 1987	NRC forwards request for additional information regarding facility modified control room habitability system (letter from G. Kalman, NRC, to G. C. Andognini, SMUD).
December 17, 1987	SMUD forwards investigations of cable issues (letter from G. A. Coward, SMUD, to F. J. Miraglia, NRC).
December 23, 1987	NRC requests assessment of management and personnel considerations surrounding findings of April 1-May 16, 1986 inspection within 30 days to assist NRC in determining extent of enforcement action. Level of utility confidence in current management questioned (letter from J. B. Martin, NRC, to G C. Andognini, SMUD).
December 23, 1987	SMUD forwards information regarding backup indications and controls following loss of ICS/NNI system power (letter from G. A. Coward, SMUD, to F. J. Miraglia, NRC).
December 23, 1987	SMUD submits supplemental application, proposed Amendment 155, establishing new set of lower limits of detection (application from J. F. Firlit, SMUD, to F. J. Miraglia, NRC).
December 24, 1987	SMUD forwards formal responses to NRC questions from exit meeting on December 15, 1987, that concluded inspection of utility response to IE Bulletin 79-27 (letter from J. F. Firlit, SMUD, to F. J. Miraglia, NRC).
December 27, 1987	SMUD forwards Revision 5 to administrative procedure AP.310, "Offsite Dose Calculation Manual," for review to support evaluation of proposed Amendment 155 (letter from G. C. Andognini, SMUD, to F. J. Miraglia, NRC).
December 29, 1987	SMUD forwards listed reports regarding vibration on TDI emergency diesel engines (letter from G. A. Coward, SMUD, to F. J. Miraglia, NRC).
December 31, 1987	SMUD forwards response to request for results of chemical analysis and material testing of fasteners (letter from G. C. Andognini, SMUD, to F. J. Miraglia, NRC).

January 4, 1988	SMUD forwards engineering summary report for 16 TDI phase I diesel generator components containing detailed information on Design Review/Quality Revalidation Program. Vibration problems with turbocharger support bracket are resolved (letter from G. A. Coward, SMUD to F. J. Miraglia, NRC).
January 5, 1988	SMUD advises that additional modifications to control room/technical support center HVAC system needed to improve reliability and operability (letter from G. C. Andognini, SMUD, to F. J. Miraglia, NRC).
January 7, 1988	SMUD forwards supplemental information to radioactive liquid effluent system description (letter from G. C. Andognini, SMUD, to F. J. Miraglia, NRC).
January 12, 1988	NRC notifies SMUD of completion of review of November 11, 1987 emergency plan review, including classification and response during December 16, 1987 meeting and December 6, 1988 telephone conversation. Emergency plan, as changed, meets 10 CFR 50.47(b) standards and 10 CFR 50, Appendix E requirements (letter from R. F. Fish, NRC, to G. C. Andognini, SMUD).
January 13, 1988	SMUD proposes conditions for CR/TSC habitability conditions (letter from G. C. Andognini, SMUD, to F. J. Miraglia, NRC).
January 13, 1988	SMUD forwards radioactive liquid effluent system evaluation demonstrating plant capabilities for limiting radioactive liquid releases (letter from G. C. Andognini, SMUD, to F. J. Miraglia, NRC).
January 19, 1988	SMUD forwards response to NUREG-1275, "Operating Experience Feedback Report - New Plants" (letter from J. F. Firlit, SMUD, to F. J. Miraglia, NRC).
January 20, 1988	NRC requests establishment of two hold points during heatup and approach to criticality and that all prerequisites for proceeding beyond each hold point be completed (letter from J. B. Martin, NRC, to G. C. Andognini, SMUD).
January 22, 1988	SMUD provides information on TDI diesel generator backup air system regarding design, operation, and testing (letter from B. G. Croley, SMUD, to F. J. Miraglia, NRC).
January 22, 1988	SMUD forwards November/December update to "Wire and Cable Program Report," per May 6, 1987 meeting (letter from G C. Andognini, SMUD, to F. J. Miraglia, NRC).

January 25, 1988	NRC forwards Augmented System Review Test Program Followup Inspection Report 50-312/87-29 (letter from D. M. Crutchfield, NRC, to G. C. Andognini, SMUD).
January 27, 1988	SMUD forwards Revision 1 to special test procedure STP.961, "Loss of Offsite Power" (letter from J. F. Ferlit, SMUD, to G. Kalman, NRC).
February 10, 1988	SMUD responds to NUREG-0737, Item III.D.3.4 (letter from G. C. Andognini, SMUD, to F. J. Miraglia, NRC).
February 25, 1988	SMUD submits proposed Amendment 164 regarding revised condition for storage of chlorine on site (letter from G. C. Andognini, SMUD, to F. J. Miraglia, NRC).

APPENDIX B

REFERENCES

American National Standards Insitute/American Concrete Institute, ANSI/ACI Standard 349, "Code Requirements for Nuclear Safety Related Concrete Structures."

American National Standards Institute/American Nuclear Society, ANSI/ANS Standard 59.3, "Safety Criteria for Control Air Systems."

---, ANSI Standard B31.1.

American National Standards Institute/Instrument Society of America, ANSI/ISA Standard S7.3, "Quality Standard for Instrument Air."

Babcock and Wilcox Owners Group, BAW-1919, Revision 5, "B&W Owners Group Safety and Performance Improvement Program," July 1987.

Institute of Electrical and Electronics Engineers, Standard 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," 1971.

---, Standard 308, "Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations," 1974.

---, Standard 323, "Qualifying Class 1E Equipment for Nuclear Power Generating Stations," 1974.

---, Standard 344, "Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," 1975.

---, Standard 384, "Standard Criteria for Independence of Class 1E Equipment and Circuits," 1974.

U.S. Nuclear Regulatory Commission, AEOD/C701, "Case Study Report on Air Systems Problems at U.S. Light Water Reactors,"

---, Generic Letter 82-33.

---, IE Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation," November 30, 1979.

---, IE Circular 79-02, "Failure of 120-Volt AC Power Supplies," January 11, 1979.

---, IE Information Notice 80-07, March 7, 1980.

---, IE Information Notice 83-17.

---, Memorandum dated July 7, 1987 from F. O. Coffman to G. W. Knighton.

---, NUREG-0696, "Functional Criteria for Emergency Response Facilities," Final Report, February 1981.

---, NUREG-0700, "Guidelines for Control Room Design Reviews," September 1981.

---, NUREG-0737, "Clarification of TMI Action Plan Requirements," November 1980; Supplement 1, "Requirements for Emergency Response Capability," January 1983.

---, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," LWR Edition, July 1981.

---, NUREG-1195, "Loss of Integrated Control System Power and Overcooling Transient at Rancho Seco on December 26, 1985," February 1986.

---, NUREG-1216, "Safety Evaluation Report Related to the Operability and Reliability of Emergency Diesel Generators Manufactured by Transamerica Delaval, Inc.," August 1986.

---, NUREG-1275, "Operating Experience Feedback Report: New Plants," July 1987.

---, NUREG/CR-0660, "Enhancement of On-site Emergency Diesel Generator Reliability," February 1979.

APPENDIX C

ACRONYMS AND OTHER INITIALISMS

ABT	automatic bus transfer
ACI	American Concrete Institute
ADV	atmospheric dump valve
AFW	auxiliary feedwater
AGM	Assistant General Manager
ANSI	American National Standards Institute
AP	administrative procedure
ASME	American Society of Mechanical Engineers
ASRTP	Augmented System Review and Test Program
ATF	automatic transmission fluid
ATOG	abnormal transient operating guideline
BTP	Branch Technical Position
B&W	Babcock and Wilcox
BWOG	Babcock and Wilcox Owners Group
CCG	Card Control Group
CCU	central control unit
CCW	component cooling water
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
CIDR	Construction Inspection Data Report
CP	casualty procedure
CR	control room
CRT	cathode-ray tube
CRTS	cable and raceway tracking system
CST	condensate storage tank
CSU	central switching unit
DBA	design-basis accident
DBE	design-basis earthquake
DCN	design change notice
DCRDR	detailed control room design review
DDAC	diesel-driven air compressor
DFCA	deterministic failure consequence analysis
DGB	diesel generator building
DR	design review
DRQR	design review and quality revalidation
ECC	emergency core cooling
EDG	emergency diesel generator
EFIC	emergency feedwater initiation and control
EM	electrical maintenance
EMOV	electromagnetic operating valve

EUP	emergency operating procedure
EP	emergency procedure
E/P	electric/pneumatic
EPIP	emergency plan implementing procedure
ESF	engineered safety feature
ESFAS	emergency safety features actuation system
ESFVS	engineered safety features ventilation system
FCV	feed control valve
FOGG	feed only good generator
FSAR	Final Safety Analysis Report
GDC	General Design Criteri(on)(a)
HEPA	high efficiency particulate air
HPI	high-pressure injection
HVAC	heating, ventilation, and air conditioning
IAS	instrument air system
I&C	instrumentation and control
ICS	integrated control system
IDADS	interim data acquisition and display system
IEEE	Institute of Electrical and Electronics Engineers
IIRG	Incident Investigation/Review Group
INEL	Idaho National Engineering Laboratory
INPO	Institute of Nuclear Power Operations
ISA	Instrument Society of America
LCO	limiting condition for operation
LER	Licensee Event Report
LLD	lower limits of detection
LOCA	loss-of-coolant accident
LOOP	loss of offsite power
LTOP	low-temperature, overpressure protection
MCC	motor control center
MFW	main feedwater
MSL	main steamline
MSLFL	main steamline failure logic
MSSV	main steam safety valve
NGS	nitrogen gas system
NNI	non-nuclear instrumentation
NPS	Nuclear Power Services
NRC	U.S. Nuclear Regulatory Commission
NSEB	nuclear service electric building
OBE	operating-basis earthquake
ODCM	Offsite Dose Calculation Manual
OTSG	once-through steam generator

PASS	postaccident sampling system
PC	printed circuit
PGP	procedures generation package
P&ID	piping and instrumentation diagram
PM	preventive maintenance
PP&MIP	Plant Performance and Management Improvement Program
PRA	probabilistic risk assessment
PSM	power supply monitor
P-T	pressure-temperature
QA	quality assurance
QC	quality control
QR	quality revalidation
RCP	reactor coolant pump
RCS	reactor coolant system
RECM	Radiological Effluent Control Manual
REMP	Radiologicl Environmental Monitoring Program
RG	regulatory guide
RO	Reactor Operator
RPS	reactor protection system
RSTS	Rancho Seco Technical Specifications
RTS	Recommendation Tracking System
SAIC	Science Applications International Corporation
SER	Safety Evaluation Report
SFAS	safety features actuation system
SMUD	Sacramento Municipal Utility District
SP	surveillance procedure
SPDS	safety parameter display system
SPIP	Safety and Performance Improvement Program
SRO	Senior Reactor Operator
SRP	Standard Review Plan
SRTP	Systems Review and Test Program
SSE	safe shutdown earthquake
STA	Shift Technical Advisor
STP	special test procedure
STS	Standard Technical Specifications
SUFW	startup feedwater
TAP	Transient Assessment Program
TBV	turbine bypass valve
TDAFW	turbine-driven auxiliary feedwater
TDD	time delay on dropout
TDI	Transamerica Delaval, Inc.
TIE	trip interface equipment
TMI	Three Mile Island
TS	Technical Specifications
TSC	technical support center
UPS	uninterruptible power supply
USAR	"Rancho Seco Nuclear Generating Station Updated Safety Analysis Report"

APPENDIX D

NRC STAFF CONTRIBUTORS

Name	Organization
I. Ahmed	Electrical Systems Branch*
W. Ang	Reactor Projects Branch**
L. Beltracchi	Reliability and Human Factors Branch†
R. Bevan	Project Directorate V*
M. Caruso	Division of Reactor Projects III, IV, V and Special Projects*
M. Cillis	Emergency Preparedness and Radiological Protection Branch**
J. Dyer	Special Inspection Branch*
R. Fish	Emergency Preparedness and Radiological Protection Branch**
M. Hartzman	Mechanical Engineering Branch*
R. Jones	Reactor Systems Branch*
G. Kalman	Project Directorate V*
N. Le	Performance Evaluation Branch*
J. Miller	Technical Specifications Branch*
L. Miller	Reactor Projects Branch**
J. Persensky	Human Factors Assessment Branch*
I. Spickler	Radiation Protection Branch*
R. Stevens	Instrumentation and Control Systems Branch*
J. Stewart	Instrumentation and Control Systems Branch*
N. Thompson	Structural and Geosciences Branch*
C. Trammell	Project Directorate V*
E. Tomlinson	Project Directorate IV*
F. Witt	Chemical Engineering Branch*

*Office of Nuclear Reactor Regulation

**Region V

†Office of Nuclear Regulatory Research

NRC FORM 335 (2-84) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

SEE INSTRUCTIONS ON THE REVERSE

1. REPORT NUMBER (Assigned by TIDC, add Vol. No., if any)
NUREG-1286
Supplement No. 1

2. TITLE AND SUBTITLE
Safety Evaluation Report related to the restart of Rancho Seco Nuclear Generating Station, Unit 1, following the event of December 26, 1985

3. LEAVE BLANK

4. DATE REPORT COMPLETED
MONTH: March
YEAR: 1988

5. AUTHOR(S)

6. DATE REPORT ISSUED
MONTH: March
YEAR: 1988

7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Division of Reactor Projects - III, IV, V
and Special Projects
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

8. PROJECT/TASK/WORK UNIT NUMBER

9. FIN OR GRANT NUMBER

10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Same as 7. above

11a. TYPE OF REPORT
Safety Evaluation Report

b. PERIOD COVERED (Inclusive dates)

12. SUPPLEMENTARY NOTES
Docket No. 50-312

13. ABSTRACT (200 words or less)

On December 26, 1985, the Rancho Seco Nuclear Generating Station experienced a reactor trip from 76% power, followed by a rapid overcooling transient and automatic initiation of the safety features actuation system. The unit has remained shut down since that time. In response to confirmatory letters from the NRC Region V Administrator, the licensee, Sacramento Municipal Utility District (SMUD), submitted the "Rancho Seco Action Plan for Performance Improvement" in July 1986. Since then, the licensee has submitted revisions to that action plan and numerous other documents and information to support a return of Rancho Seco to power operation. The NRC staff reviewed the licensee's submittals and other information made available to the staff in support of a restart of Rancho Seco. In October 1987, the NRC staff issued a Safety Evaluation Report (NUREG-1286) relating to the restart of Rancho Seco. Since then, the staff has completed its review of all other issues relating to the restart effort. The results of this more recently completed review work are contained in this Supplement No. 1 to NUREG-1286.

14. DOCUMENT ANALYSIS - a. KEYWORDS/DESCRIPTORS
Safety Evaluation Report; Operating Reactors; Loss of Feedwater; Rancho Seco Nuclear Generating Station; emergency feedwater initiation and control; TDI diesels; non-nuclear instrumentation system; integrated control system; Babcock and Wilcox Owners Group

b. IDENTIFIERS/OPEN ENDED TERMS

15. AVAILABILITY STATEMENT
Unlimited

16. SECURITY CLASSIFICATION
(This page) Unclassified
(This report) Unclassified

17. NUMBER OF PAGES

18. PRICE

8804080230

* U.S. GOVERNMENT PRINTING OFFICE: 1988-202-292:80005

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