

---

---

# Loss of Integrated Control System Power and Overcooling Transient at Rancho Seco on December 26, 1985

---

---

U.S. Nuclear Regulatory  
Commission



8603100574 860228  
PDR ADDCK 05000312  
S PDR

## 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 Technical Information and Document Control, 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.

---

# Loss of Integrated Control System Power and Overcooling Transient at Rancho Seco on December 26, 1985

---

Manuscript Completed: February 1986  
Date Published: February 1986

U.S. Nuclear Regulatory Commission  
Washington, D.C. 20555



## ABSTRACT

On December 26, 1985, Rancho Seco Nuclear Generating Station, located in Clay, California, about 25 miles southeast of Sacramento, experienced a loss of dc power within the integrated control system (ICS) while the plant was operating at 76 percent power. The plant is owned by the Sacramento Municipal Utility District (SMUD). Following the loss of ICS dc power, the reactor tripped on high reactor coolant system (RCS) pressure followed by a rapid overcooling transient and automatic initiation of the safety features actuation system on low RCS pressure. The overcooling transient continued until ICS dc power was restored 26 minutes after its loss. The fundamental causes for this transient were design weaknesses and vulnerabilities in the ICS and in the equipment controlled by that system. These weaknesses and vulnerabilities were not adequately compensated by other design features, plant procedures or operator training. These weaknesses and vulnerabilities were largely known to SMUD and the NRC staff by virtue of a number of precursor events and through related analyses and studies. Yet, adequate plant modifications were not made so that this event would be improbable, or so that its course or consequences would be altered significantly. The information was available and known which could have prevented this overcooling transient; but in the absence of adequate plant modifications, the incident should have been expected. The report includes findings and conclusions of the NRC Incident Investigation Team sent to Rancho Seco by the NRC Executive Director for Operations in conformance with NRC's recently established Incident Investigation Program.

## TABLE OF CONTENTS

	<u>Page</u>
Abstract . . . . .	iii
List of Figures and Tables . . . . .	viii
The NRC Team for the Rancho Seco Event of December 26, 1985 . . . . .	x
Acronyms and Abbreviations . . . . .	xi
1. INTRODUCTION . . . . .	1-1
2. DESCRIPTION OF FACT FINDING EFFORTS . . . . .	2-1
2.1 General Approach . . . . .	2-1
2.2 Interviews and Meetings . . . . .	2-1
2.3 Plant Data . . . . .	2-2
2.4 Quarantined Equipment and Troubleshooting Procedures. . . . .	2-2
3. SYSTEM DESCRIPTIONS . . . . .	3-1
3.1 Integrated Control System . . . . .	3-1
3.1.1 Fundamental Control Scheme. . . . .	3-2
3.1.2 Block Diagram . . . . .	3-3
3.1.3 Output Signals. . . . .	3-4
3.1.4 Loss of ICS dc Power. . . . .	3-5
3.1.5 Restoration of ICS dc Power . . . . .	3-5
3.1.6 ICS Power Supplies and Distribution System. . . . .	3-6
3.2 Auxiliary Feedwater System . . . . .	3-7
3.3 Main Feedwater System . . . . .	3-9
3.4 Once-Through Steam Generators . . . . .	3-10
3.5 Main Steam System . . . . .	3-11
3.6 Makeup/High Pressure Injection System . . . . .	3-12
4. NARRATIVE OF THE INCIDENT . . . . .	4-1
4.1 Plant Status and Oncoming Shift . . . . .	4-1
4.2 Loss of the Integrated Control System DC Power. . . . .	4-1
4.3 Plant Trip and RCS Cooldown . . . . .	4-2
4.4 SFAS Actuation, Continued Plant Cooldown and Partial Depressurization . . . . .	4-3
4.5 Excessive Plant Cooldown and Partial Repressurization . . . . .	4-5
4.6 Restoration of ICS DC Power and Plant Stabilization . . . . .	4-8

TABLE OF CONTENTS (cont.)

	<u>Page</u>
5. EQUIPMENT PERFORMANCE . . . . .	5-1
5.1 Integrated Control System . . . . .	5-1
5.1.1 Root Cause Determination . . . . .	5-1
5.2 AFW(ICS) Flow Control System . . . . .	5-4
5.2.1 Component Description. . . . .	5-6
5.2.2 Root Cause Determination . . . . .	5-6
5.3 AFW Manual Isolation Valve . . . . .	5-7
5.3.1 Component Description. . . . .	5-7
5.3.2 Root Cause Determination . . . . .	5-8
5.4 Makeup Pump. . . . .	5-9
5.4.1 Component Description. . . . .	5-11
5.4.2 System Response and Interactions . . . . .	5-11
5.5 Pressurizer . . . . .	5-12
6. PERSONNEL PERFORMANCE . . . . .	6-1
6.1 Introduction . . . . .	6-1
6.2 Shift Staffing . . . . .	6-1
6.3 Event Recognition. . . . .	6-3
6.4 Adequacy of Procedures . . . . .	6-4
6.5 Compliance With Procedures . . . . .	6-8
6.6 Role of the Shift Technical Advisor. . . . .	6-10
6.7 Licensed Operator Training . . . . .	6-11
6.8 Nonlicensed Operator Training. . . . .	6-12
6.9 Radiation Protection and Emergency Plan. . . . .	6-13
7. PRECURSORS TO THE DECEMBER 26, 1986 INCIDENT AT RANCHO SECO AND RELATED NRC AND SMUD ACTIONS. . . . .	7-1
7.1 Response of B&W Plants to Failures in the ICS and NNI . . . . .	7-1
7.1.1 The Rancho Seco "Lightbulb Incident" . . . . .	7-1
7.1.2 The first Rancho Seco Loss of ICS Incident . . . . .	7-2
7.1.3 BAW-1564, "Integrated Control System Reliability Analysis" . . . . .	7-3
7.1.4 IE Bulletin 79-27, "Loss of Non-Class-1E- Instrumentation and Control Power System Bus During Operation" . . . . .	7-5
7.1.5 NUREG-0667, "Transient Response of Babcock & Wilcox-Designed Reactors". . . . .	7-11
7.1.6 March 19, 1984 Partial Loss of NNI at Rancho Seco . . . . .	7-15
7.1.7 USI A-47, "Safety Implications of Control Systems". . . . .	7-17

TABLE OF CONTENTS (cont.)

	<u>Page</u>
7.2 Emergency Feedwater Initiation and Control . . . . .	7-19
7.2.1 System Purpose . . . . .	7-19
7.2.2 System Description . . . . .	7-19
7.2.3 Significance of Absence of EFIC . . . . .	7-20
7.2.4 Regulatory History . . . . .	7-20
8. SIGNIFICANCE OF THE INCIDENT . . . . .	8-1
8.1 Introduction . . . . .	8-1
8.2 Pressurized Thermal Shock . . . . .	8-1
8.3 Analyses . . . . .	8-2
8.3.1 Comparison with the "Lightbulb Incident" . . . . .	8-2
8.3.2 Generic PTS Analysis . . . . .	8-2
8.3.3 FSAR Accident Analysis. . . . .	8-4
8.3.4 Consequences of the Incident Under Alternate Conditions . . . . .	8-5
9. ADDITIONAL ISSUES. . . . .	9-1
9.1 Main Steam Line Failure Logic System . . . . .	9-1
9.1.1 Purpose of the MSFL System . . . . .	9-1
9.1.2 Description of the MSFL System . . . . .	9-1
9.1.3 Safety Classification . . . . .	9-2
9.2 AC Power-Dependency of the AFW System . . . . .	9-2
10. Conclusions . . . . .	10-1
10.1 Principal Findings and Conclusions. . . . .	10-1
10.2 Other Findings and Conclusions. . . . .	10-6

APPENDIX

Memorandum from J. W. Dircks, Executive Director for Operations, to the Commission, "Investigation of December 26, 1985 Event at Rancho Seco Will Be Conducted by an Incident Investigation Team (IIT)" . . . . .	A-1
--	-----

LIST OF FIGURES AND TABLES

<u>Figures</u>	<u>Page</u>
3.1 Rancho Seco basic plant control concept . . . . .	3-15
3.2 The Rancho Seco integrated control system . . . . .	3-16
3.3 Equipment diagram -- control of turbine bypass valve A. . . . .	3-17
3.4 Typical ICS "hand/auto" control system. . . . .	3-18
3.5 ICS direct current power supplies . . . . .	3-19
3.6 ICS +/-24 Vdc buses (ICS cabinet #3). . . . .	3-20
3.7 ICS power switches S1 and S2 . . . . .	3-21
3.8 Auxiliary feedwater system (simplified) . . . . .	3-22
3.9 Main feedwater system (simplified) . . . . .	3-23
3.10 Once-through steam generators flow paths and level indication . . . . .	3-24
3.11 Main steam system (simplified). . . . .	3-25
3.12 Makeup/high pressure injection system (simplified). . . . .	3-26
4.1 RCS pressure/pressurizer level from 4 a.m. to 5 a.m. on December 26, 1985 . . . . .	4-19
4.2 RCS pressure/temperature ( $T_{ave}$ )/RCS saturation temperature ( $T_{sat}$ ) on reactor trip from 4 a.m. to 5 a.m. on December 26, 1985 . . . . .	4-20
4.3 Auxiliary feedwater flowrates on reactor trip, December 26, 1985 . . . . .	4-21
4.4 HPI and makeup injection flow rates on reactor trip, December 26, 1985 . . . . .	4-22
4.5 Full-range OTSG levels on reactor trip, December 26, 1985 . . . . .	4-23
4.6 Comparison of reactor pressure-temperature with B&W PTS and NDT Technical Specification limits. . . . .	4-24
5.1 AFW(ICS) flow control valve . . . . .	5-14
5.2 A AFW(ICS) flow control valve(FV-20527) . . . . .	5-15
5.3 AFW(ICS) flow control valve manual operator . . . . .	5-16
5.4 Damage to the A AFW(ICS) flow control valve . . . . .	5-17
5.5 AFW manual isolation valve . . . . .	5-18
5.6 AFW manual isolation valve (FWS-063) upper bearing. . . . .	5-19
5.7 Makeup pump lower casing . . . . .	5-20
5.8 Makeup pump impeller and wear rings . . . . .	5-21
6.1 Switches S1 and S2 in the tripped (OFF) position. . . . .	6-16
6.2 Position indication on AFW(ICS) flow control valve. . . . .	6-17
6.3 A AFW(ICS) flow control valve (FV-20527). . . . .	6-18
7.1 Precursors to the December 26, 1985 incident . . . . .	7-26
8.1 Overcooling incidents at Rancho Seco. . . . .	8-7
8.2 Critical valves of pressure and $T_f - RT_{NDT}$ for crack initiation in reactor vessel . . . . .	8-8
8.3 Temperatures versus time--ICS power supply failure with feedwater to both steam generators. . . . .	8-9



List of Figures and Tables (Cont.)

<u>Tables</u>	<u>Page</u>
2.1 Interviews and Meetings Conducted by the Rancho Seco Incident Investigation Team . . . . .	2-5
4.1 Chronological Sequence of Events . . . . .	4-11
7.1 Chronology of Precursor Events and Related Actions . . . . .	7-24

THE NRC TEAM FOR THE RANCHO SECO INCIDENT ON DECEMBER 26, 1985:

Frederick J. Hebdon, Team Leader  
Henry A. Bailey  
J. T. Beard  
Ronald B. Eaton  
Gordon E. Edison

TECHNICAL EDITOR:

Walter E. Oliu

INPO OBSERVER:

The NRC has proposed to the Institute of Nuclear Power Operations (INPO) that an INPO representative participate in the investigation of significant operating events as a member of an Incident Investigation Team. Although this concept continues under discussion, in order to gain further knowledge and insight regarding this activity, INPO sent a staff engineer to observe the Team's investigation of the incident at Rancho Seco. The INPO observer participated in the Team's activities, but was not a party to the Team's findings.

## ACRONYMS AND ABBREVIATIONS

ABT	automatic bus transfer
ac	alternating current
ADV	atmospheric dump valves
AEOD	Office for Analysis and Evaluation of Operational Data (NRC)
AFW	auxiliary feedwater
ANO-1	Arkansas Nuclear One, Unit 1
AO	auxiliary operator
ASME	American Society of Mechanical Engineers
ATOG	Abnormal Transient Operating Guidelines
BAW	Babcock & Wilcox
B&W	Babcock & Wilcox
Btu	British thermal units
BWR	boiling water reactor
BWST	borated water storage tank
CR-3	Crystal River Unit 3
CST	condensate storage tank
dc	direct current
DHR	decay heat removal
DOL	Division of Licensing (NRC)
DST	Division of Safety Technology (NRC)
EA	equipment attendant
ECCS	emergency core cooling system
EDO	Executive Director for Operations (NRC)
EFIC	emergency feedwater initiation and control (system)
EHC	electro-hydraulic control
ENS	Emergency Notification System
EOP	Emergency Operating Procedures
FSAR	Final Safety Analysis Report
FMEA	failure modes and effect analysis
FW	feedwater
gpm	gallons per minute
HP	high pressure
HPI	high pressure injection
HVAC	heating, ventilation and air conditioning
I&C	instrumentation and control
ICS	integrated control system
ICSB	Instrumentation and Control Systems Branch (NRC)
IDADS	interim data acquisition display system
IE	Office of Inspection and Enforcement (NRC)
IIT	Incident Investigation Team (NRC)
INPO	Institute of Nuclear Power Operations
LOCA	loss-of-coolant accident
LP	low pressure
LPI	low pressure injection
MFW	main feedwater

MPC	maximum permissible concentration
MSFL	main steamline failure logic
MSIV	main steam isolation valve
MUT	makeup tank
MWe	megawatt (electric)
NNI	non-nuclear instrumentation
NPSH	net positive suction head
NRC	U.S. Nuclear Regulatory Commission
NRR	Office of Nuclear Reactor Regulation (NRC)
NSSS	nuclear steam system supplier
OJT	on-the-job training
ORNL	Oak Ridge National Laboratory
OTSG	once-through steam generator
PPH	power plant helper
PPS	plant protection system
psi	pounds per square inch
psig	pounds per square inch gauge
PST	Pacific Standard Time
PTS	pressurized thermal shock
PWR	pressurized water reactor
QA	quality assurance
RCP	reactor coolant pump
RCS	reactor coolant system
rpm	revolutions per minute
Rx	reactor
SAR	Safety Analysis Report
SER	Safety Evaluation Report
SFAS	safety features actuation system
SMUD	Sacramento Municipal Utility District
SPDS	safety parameter display system
SRO	Senior Reactor Operator
SS	Shift Supervisor
STA	Shift Technical Advisor
TAP	Task Action Plan
T <sub>ave</sub>	average temperature
TBV	turbine bypass valves
TMI	Three Mile Island
T <sub>sat</sub>	saturation temperature
TSC	Technical Support Center
USI	unresolved safety issue
V	voltage
Vac	ac voltage
Vdc	dc voltage

## 1. INTRODUCTION

The Rancho Seco Nuclear Generating Station, operated by the Sacramento Municipal Utility District (SMUD) is a 916-MWe Babcock & Wilcox (B&W)-designed pressurized water reactor located in Clay, California, about 25 miles southeast of Sacramento. The plant received an NRC operating license in 1974.

At 4:14 a.m. on December 26, 1985, the plant was operating at 76 percent power, when a loss of integrated control system (ICS) dc power occurred as a result of a single failure. The loss of dc power to the ICS (a nonsafety-related system) caused a number of feedwater and steam valves to reposition automatically and also caused the loss of remote control of the affected valves from the control room. In addition, the main feedwater (MFW) pump turbines slowed to minimum speed and the auxiliary feedwater (AFW) pumps started. The immediate result was a reactor coolant system (RCS) undercooling condition that resulted in the reactor tripping on high pressure. The reactor trip was followed by an overcooling condition that resulted in safety features actuation and excessive RCS cooldown.

The operators were not immediately able to restore dc power within the ICS. As a result, nonlicensed operators were sent to isolate the affected steam and feedwater valves locally with handwheels. During the first 7 minutes of the incident, the excessive steam and feedwater flows resulted in a rapid RCS cooldown of over 100 °F. The pressurizer emptied and a small bubble formed in the reactor vessel head. The RCS cooldown continued and the RCS depressurized to about 1064 psig and then began to repressurize. This repressurization resulted in the RCS entering the B&W-designated pressurized thermal shock (PTS) region. The atmospheric dump valves and turbine bypass valves were isolated within 9 minutes after the reactor trip. However, the operators experienced difficulty closing the ICS-controlled AFW flow control valves. One of the AFW flow control valves was finally shut; however, the second AFW flow control valve was damaged and failed open. The associated AFW manual isolation valve was found to be stuck open. Therefore, both AFW pumps continued to feed and overflow one steam generator. Since the plant has no main steam isolation valves, water began to overflow into the main steam lines.

About 26 minutes after the reactor trip, the operators restored power within the ICS by reclosing two switches in an ICS cabinet. The operators were then able to close the open AFW flow control valve from the control room, which stopped the RCS cooldown, and started stabilizing the plant. The RCS had cooled down a total of 180 °F in this 26-minute period.

While changing a valve lineup in the suction of the pump used to supply RCS makeup (makeup pump), the last suction valve to the makeup pump was inadvertently shut. This resulted in the overheating and destruction of the makeup pump. About 450 gallons of contaminated water were spilled on the floor. This failure did not directly affect the incident since a high pressure injection (HPI) pump was available to supply RCS makeup. In addition, the spilled water did not result in any significant onsite or offsite radioactivity release or personnel dose.

Operators later stabilized the plant and brought it to a cold shutdown without a significant release of radioactivity to the environment and without significant additional damage to plant equipment. Because of the potential significance of the event, an NRC Team was sent to the site on December 27 and started their investigation of the incident on December 28. The five-member Team was selected on the basis of their knowledge and experience in the fields of reactor systems, reactor operations, human factors, and instrumentation and control systems. The Team was directed to: (a) determine the facts of what happened; (b) identify the probable cause as to why it happened; and (c) make appropriate findings and conclusions which would form the basis for any necessary follow-on actions. A specific focus of the Team was on the design and response of the ICS, and operator performance and training as they related to the loss of ICS during the incident. The scope of this fact-finding effort was limited to the circumstances surrounding the December 26, 1985 incident, including operator and NRC actions, equipment damage and malfunctions, equipment maintenance and testing history, and regulatory involvement. This report provides the results of the Team's investigation.

Section 2 describes the methods used by the Team to collect and evaluate information about the event. Section 3 provides a description of several key systems (e.g., ICS) that were involved in the incident. Section 4 provides a narrative description and detailed sequence of events, which were reconstructed from an analysis of operator interviews and logs, event recorders, and system descriptions.

Section 5 discusses the performance of plant equipment involved in the event and describes the results of the root cause determinations.

Section 6 discusses personnel performance during the incident. The issues addressed include shift staffing, event recognition, emergency operating procedures, compliance with procedures, training, and the role of the Shift Technical Advisor.

Section 7 discusses the precursors to the incident and associated SMUD and NRC staff actions. This section includes the regulatory history associated with loss of ICS power and with the emergency feedwater initiation and control (EFIC) system (a new system proposed by SMUD for future installation at Rancho Seco).

Section 8 assesses the safety significance of the incident. The incident is compared with an earlier (1978) overcooling event at Rancho Seco, the plant Final Safety Analysis Report (FSAR) analysis, and generic pressurized thermal shock analyses. The possible consequences of this event under alternate operator actions were also considered.

Section 9 addresses two peripheral issues that were not directly relevant to the incident, but were part of the Team's investigation.

Finally, Section 10 presents the Team's findings and conclusions, which are based on information available to the Team at the time this report was written.

## 2 DESCRIPTION OF FACT FINDING EFFORTS

### 2.1 General Approach

The investigative methods used by the Rancho Seco Incident Investigation Team (the Team) were based on the experience and general methods used by the Incident Investigation Team for the Davis-Besse event of June 9, 1985. To assure continuity and consistency in Team activities, one member from the Davis-Besse Team also served on the Rancho Seco Team.

The Rancho Seco Team was tasked to (a) determine the facts surrounding the incident, (b) identify the probable cause of why it happened, and (c) make appropriate findings and conclusions which would form the basis for any necessary follow-on actions. The Team was directed to specifically focus on the design and response of the integrated control system (ICS) and on operator performance and training as they related to the loss of ICS during the event.

The Team collected and evaluated information to determine the sequence of operator and equipment responses during the event and the causes of equipment malfunctions. The sequence of these responses was determined primarily by interviewing personnel who were at the plant during the event and by reviewing plant data for the period immediately preceding and during the event. The Team also examined the equipment which malfunctioned, the equipment that was crucial to mitigating the transient, and control room instrumentation and controls.

As is true of all commercial nuclear power plants, a considerable amount of information on plant response and specific equipment actuation can be obtained from records automatically generated in the form of analog recordings and digital printouts. These records indicate the chronological sequence for such occurrences as the starting and stopping of pumps and the opening and closing of valves, as well as the time response of key plant parameters. By correlating plant records with personnel statements on actions and observations, the Team was able to compile a detailed profile of key aspects of the event.

The equipment which malfunctioned and contributed to the event was quarantined so that troubleshooting could be performed systematically and so that, as a result, information on the root causes of each malfunction would not be lost or destroyed.

### 2.2 Interviews and Meetings

The Team placed a high priority on interviewing personnel on duty at the time of the event to learn about the actions they took and the observations they made. The Team recognized that the quicker these interviews could be held, the more information those being interviewed would remember. The Team held meetings with Sacramento Municipal Utility District (SMUD) personnel to obtain information on the sequence of events and to agree upon a course of action for troubleshooting the quarantined equipment. The Team subsequently interviewed SMUD and U.S. Nuclear Regulatory Commission (NRC) staff members concerning a

number of regulatory issues that had a direct impact on the cause and course of the event.

All interviews and meetings were recorded by stenographers who prepared typed transcripts. A record was not made of discussions between the Team and SMUD personnel about routine administrative matters (e.g., schedules).

The formal fact-finding effort began on the morning of December 28, 1985. SMUD personnel presented an overview of their understanding of the incident and the specific design features of the Rancho Seco plant important to understanding the incident. Interviews with operating personnel also began on December 28, 1985. The general approach for scheduling interviews was to talk to personnel in decreasing order of their seniority within the shift, beginning with the Shift Supervisor and proceeding to those less senior. The rationale for this sequence was to move from general to specific information. Thus, the Team obtained information on overall plant operations before obtaining information on the detailed actions of specific operators. The scheduling of interviews and meetings was also based on the availability of personnel.

Some personnel were interviewed more than once when the Team needed additional clarifying information. Table 2.1 contains a listing of the interviews and meetings conducted by the Team.

### 2.3 Plant Data

The following plant records were used in determining the times at which key events occurred during the transient:

1. Strip Charts from trend recorders
2. Interim Data Acquisition Display System (IDADS) printout
3. Analog curves generated from the digital information from the IDADS
4. Logs maintained by operators and security personnel.

Unfortunately, one of the two plant computers was out of service before and during the event. Consequently, some data normally supplied from that computer to the IDADS were not available.

IDADS maintains a record of plant parameters for event analyses. Key plant variables are scanned and recorded at various intervals. Data from this system were available to the Team both in tabular form and, for selected variables, in the form of graphs.

### 2.4 Quarantined Equipment and Troubleshooting Procedures

On December 26, 1985, NRC Region V issued two Confirmatory Action Letters verifying, among other things, that SMUD would not perform any additional work on equipment that malfunctioned during the event until the Team could review the proposed troubleshooting actions. The Team met with SMUD and Region V representatives to ensure agreement on the quarantined equipment list and to establish a course of action for determining the root causes of the equipment malfunctions. SMUD committed to perform the troubleshooting in a systematic, controlled, and well-documented manner, and to maintain adequate records on the "as-found" condition of equipment. All items that had failed during the event were initially placed on the quarantine list. Subsequently, items were removed



from the list when justified by SMUD on the basis that the failure was not related to the safety concerns of the incident.

On January 1, 1986, SMUD issued, "Transient Analysis Organization, Troubleshooting, and Equipment Repair Following 12-26-85 Transient," a document which delineated the general procedures they planned to follow for troubleshooting equipment. This document was revised after extensive discussions with the Team and subsequently issued for implementation as Revision 2 on January 4, 1986.

The general troubleshooting procedures required maintenance work orders based upon a specific troubleshooting plan for each piece of equipment. The specific troubleshooting plans contained hypotheses and probable causes of failure or abnormal operation for each piece of equipment on the quarantine list. The plans also included an analysis of information concerning the operation of the equipment during the event; a review of the maintenance, surveillance and testing history for the equipment; and plans for determining the probable causes for the equipment malfunctions observed. Finally, the plans specified where equipment vendor representatives were to be used in the troubleshooting.

Subsequent to issuance of these guidelines, troubleshooting plans were developed for each piece of equipment on the quarantine list. As a result, the as-found conditions, such as damaged components or setpoint adjustments, were documented. In addition, retention and complete traceability for components and equipment requiring replacement were maintained.

SMUD personnel agreed to notify NRC when the root cause of the malfunction or failure of a piece of equipment was determined. They also agreed that the results of the troubleshooting process, root cause determinations, and supporting engineering justification were to be submitted to the Team as soon as practical. They also agreed not to proceed with repair/corrective actions on a piece of quarantined equipment until NRC had concurred in the root cause determination. The Team did not approve each troubleshooting plan, but did review and provide extensive comments on the plans. NRC Region V personnel monitored SMUD troubleshooting efforts to ensure that both the general guidelines and the specific equipment troubleshooting plans were followed.

During early February, the Team received engineering reports from SMUD which described the results of the troubleshooting efforts and presented the engineering justification for each piece of quarantined equipment. When the Team agreed with the root cause determination, that piece of equipment was removed from the quarantine list. The information available on root causes at the time this report was prepared is discussed in Section 5.

Throughout the Team's review of the December 26, 1985 incident, SMUD personnel had considerable difficulty providing information in the detail that the Team requested. Thus, SMUD personnel repeatedly summarized data, analyses, and plans without including the actual data and analyses. As a result, the Team had to request the detailed underlying data and analyses, which subsequently were provided. This iterative process delayed the Team's onsite investigation.

It appeared to the Team that SMUD personnel found the process of troubleshooting in a highly controlled, systematic, and well-documented manner, as

proposed by the Team, to be quite different from their usual maintenance practices. This difference contributed to the difficulty that the Team experienced in reviewing the troubleshooting program.

Table 2.1 Interviews and Meetings\* Conducted by the  
Rancho Seco Incident Investigation Team

Date	Interviews/Meetings/Discussions
12/28/85	Entrance Interview
12/28/85	Interview of Shift Supervisor
12/28/85	Interview of Senior Control Room Officer
12/28/85	Interview of Control Room Operator
12/28/85	Interview of Control Room Operator
12/28/85	Interview of Equipment Attendant
12/28/85	Interview of Auxiliary Operator
12/28/85	Interview of Clearance Coordinator
12/28/85	Interview of Backup Shift Supervisor
12/29/85	Interview of Senior Resident Inspector
12/29/85	Interview of Resident Inspector (Palo Verde)
12/29/85	Interview of Assistant Operations Superintendent
12/29/85	Interview of Acting Plant Superintendent
12/29/85	Interview of Equipment Attendant
12/29/85	Interview of Equipment Attendant
12/29/85	Interview of Power Plant Helper
12/29/85	Interview of Shift Technical Advisor
12/30/85	Interview of Equipment Attendant
12/30/85	Interview of Equipment Attendant
12/30/85	Meeting with Licensee
12/31/85	Meeting with Licensee

\*Transcripts were made of all meetings and interviews listed.

Table 2.1 (continued)

Date	Interviews/Meetings/Discussions
12/31/85	Meeting with Licensee
12/31/85	Meeting with Licensee
1/2/86	Morning Status Report Meeting
1/3/86	Discussion of General Troubleshooting Guidelines
1/3/86	Morning Status Report Meeting
1/4/86	Interview of I&C Maintenance Superintendent
1/4/86	Morning Status Report Meeting
1/5/86	IIT Comments on Draft Troubleshooting Plan for the ICS
1/5/86	Status Report Update
1/6/86	Interview of Supervisor, Electrical Engineers, Sacramento Municipal Utility District (SMUD)
1/6/86	Discussion with Manager of Licensing, SMUD
1/6/86	Interview of Human Factors Personnel, SMUD
1/6/86	Morning Status Report Meeting
1/7/86	Discussion on IE Bulletin 79-27
1/7/86	Discussion of Main Steam Line Failure Logic
1/7/86	Discussion of Training Issues
1/7/86	Discussion of Troubleshooting Plans for Auxiliary Feedwater Valves FV-20527, FV-20528, FWS-063, FWS-064
1/7/86	Morning Status Report Meeting
1/8/86	Discussion of ICS Action Plan
1/8/86	Interview of Former Rancho Seco Plant Manager, SMUD
1/8/86	Interview of Consultant
1/8/86	Meeting on Human Factors Issues
1/8/86	Morning Status Report Meeting

Table 2.1 (continued)

Date	Interviews/Meetings/Discussions
1/8/86	Exit Interview
1/15/86	Interview of Director, Division of Emergency Preparedness and Engineering Response, IE
1/15/86	Interview of Branch Chief, Electrical Instrumentation and Control Systems Branch, NRR
1/15/86	Interview of former reviewer, ICSB/NRR
1/15/86	Interview of former reviewer, ICSB/NRR
1/16/86	Interview of Section Chief, Engineering Section, Reactor Operations Analysis Branch, AEOD
1/16/86	Interview of Senior Nuclear Engineer, Reactor Systems Branch, NRR
1/16/86	Interview of Systems Engineer, AEOD
1/16/86	Interview of NRC Staff (B&W Procedures)
1/17/86	Interview of Director, Operating Reactor Assessments Branch, NRR
1/17/86	Interview of Senior Task Manager, Engineering Issues Branch, NRR
2/12/86	Additional Interview of Director, Operating Reactor Assessments Staff, NRR
2/12/86	Additional Interview of Senior Task Manager, Engineering Issues Branch, NRR
2/12/86	Interview of Senior Project Manager, PWR Project Directorate #6, Division of PWR Licensing-B, NRR

### 3 SYSTEM DESCRIPTIONS

The purpose of this section is to describe the following principal plant systems that were involved in the December 26, 1985 incident: the integrated control system; auxiliary feedwater system; main feedwater system; once through steam generators; main steam system; and the makeup and high pressure injection system. The first two systems are described in greater detail than the others because they played major roles in the incident. The emergency feedwater initiation and control (EFIC) system is described separately in Section 7.2, because it is not yet operational at Rancho Seco. The descriptions are provided at the level of detail believed appropriate for a full understanding of the equipment responses during the incidents.

The methods by which equipment involved in this incident are actuated are important to an understanding of what happened and its significance. To clarify these actuation methods, the Team has adopted the following conventions to indicate that operators remotely controlled equipment (from the control room or elsewhere), that they manipulated the equipment directly, or that the equipment was actuated automatically by plant systems without operator intervention:

- o Remote (CR): Actuation of the equipment by operators from the control room (CR) or other locations remote from the equipment.
- o Manual (local): Operators physically manipulated the equipment locally.
- o Automatic: The equipment was actuated other than by the operators.

#### 3.1 Integrated Control System

The integrated control system (ICS) is a nonsafety-related system that coordinates the action of a variety of plant equipment to make the adjustments necessary to match megawatts generated to megawatts demanded by balancing steam production and steam usage. The ICS was used first on B&W-designed fossil-fueled generating plants and later adapted for use on B&W-designed nuclear plants. The ICS is essentially the same for fossil plants as for nuclear plants, with the controls that are unique to the nuclear plants (such as pressure control of the reactor coolant system) being provided by the so-called non-nuclear instrumentation (NNI) system.

The first nuclear application of the ICS was the Type 721 design which is installed in the two earliest B&W-designed plants (i.e., Oconee and Three Mile Island). The second generation of the ICS is the Type 820 design which is installed at the Rancho Seco plant and all other B&W-designed plants. These two designs of the ICS are quite similar at the functional level, but the detailed design and the actual hardware differ significantly, especially with regard to power distribution and manual control upon loss of power which are discussed below.

The following description contrasts the integrated control scheme that characterizes the ICS with the discrete, separate control schemes that characterize

other systems. This section also describes the four major portions of the ICS and the interface between the ICS and the NNI. The nature of the ICS output control signals is presented, followed by a discussion of how these output signals change upon loss and restoration of ICS power. Finally, the ICS electric power distribution system is described.

### 3.1.1 Fundamental Control Scheme

Operating nuclear power plants use three fundamental control schemes. In each of these schemes, the reactor and the steam generator are considered as a unit (i.e., the steam production portion of the plant) and the main turbine and generator are considered as another unit (i.e., the steam usage portion of the plant). The purpose of these control schemes is to match the megawatts produced (in the steam production portion) to the megawatts demanded by balancing steam production to steam usage.

In the first control scheme, the turbine generator responds initially to changes in electric demand, and the reactor and steam generator subsequently are re-adjusted to maintain the needed steam conditions. This scheme has the advantage of rapid accurate electrical output changes, but some steam flow instabilities may result.

In the second control scheme, the reactor and steam generator respond initially to changes in electrical demand, and the turbine generator are subsequently re-adjusted to satisfy the new demand. This scheme has the advantage of good plant stability, but involves a slower response to changes in electrical demand.

The third scheme, which is used at Rancho Seco, combines the first two schemes into an integrated control scheme. The objective of the combination is to take advantage of both fast plant response and good plant stability. In the ICS, steam usage (i.e., steam flow) is controlled by modulating the turbine throttle valves to maintain a constant steam header pressure. Steam production is controlled by maintaining a constant average temperature ( $T_{ave}$ ) in the reactor coolant system and modulating feedwater flow. In this control scheme, the turbine steam header pressure is used as an index of whether steam flow and steam production are in balance. On the reactor and steam generator side,  $T_{ave}$  is used as an index of whether feedwater and nuclear heat are in balance.

Figure 3.1 illustrates the fundamental control concept of the ICS at Rancho Seco. The ICS sends demand signals simultaneously to both the steam flow controls and the steam production controls. The scheme achieves fast response by initially borrowing energy from the steam generators (resulting in reduced steam pressure) and subsequently redepositing the energy as the reactor power and steam production increase. When an increase in megawatt demand occurs, the setpoint for the steam header pressure is artificially reduced temporarily. This action causes the turbine throttle valves to open further, immediately increasing steam flow and turbine generator output. As the reactor and steam generator respond to their demand signals and produce more steam, the energy borrowed is replaced as the pressure returns to the original setpoint value.

Because it employs the integrated control scheme, the Rancho Seco ICS is inherently a single, tightly interwoven, and complex system involving both feedback and anticipatory feedforward signals throughout the plant. Control schemes at

other plants (e.g., at Westinghouse and GE-designed plants) use several electrically separate and independent control systems to balance steam production and steam usage. For example, one control system maintains the turbine steam flow at a constant value; another control system matches feedwater flow to steam flow; and a third control system maintains reactor power at a constant value. The primary advantage of separate control systems is that when a single control system fails, the other control systems are electrically independent, are not affected and, therefore, tend to stabilize overall plant conditions. In contrast, when the ICS fails, the negative effects may be fed throughout the plant, causing overall plant conditions to degrade rapidly.

### 3.1.2 Block Diagram

Figure 3.2 illustrates the four major equipment subsystems of the ICS: the unit load demand; integrated master control; feedwater control; and reactor control.

The unit load demand subsystem is the primary interface between the ICS and reactor operators and includes features for load setting (i.e. demand), limiting, plant runbacks, and automatic tracking to maintain plant conditions within predetermined limits.

The integrated master control subsystem serves several purposes. First, it provides the desired electrical output power based upon the electric megawatt demand signal. Second, it maintains a constant steam header pressure. One output of the integrated master interfaces with the electro-hydraulic control unit of the turbine generator. Another output signal controls the bypass of steam around the turbine directly to the condenser (i.e., the turbine bypass valves) and controls the dump of steam to the atmosphere (i.e., the atmospheric dump valves). It also calculates the demand signal for feedwater and calculates the demand signal for reactor power. The integrated master subsystem is the master control for the feedwater control and the reactor control subsystems.

The feedwater control subsystem matches the actual feedwater flow to the feedwater demand signal from the integrated master control subsystem. The total feedwater flow is also balanced between the two once through steam generators (OTSGs) so as to maintain equal heat transfer (i.e., the returning cold leg temperatures are maintained essentially equal regardless of OTSG fouling and the number of plugged tubes). The feedwater control subsystem will receive a "cross limit" signal from the reactor control subsystem if the difference between main feedwater (MFW) flow and reactor power exceeds a predetermined limit. (A "cross limit" is an additional control signal that is produced when a controlled variable is outside the normal control range.) The feedwater control subsystem sends a "cross limit" signal to the reactor control subsystem to reduce power if the reactor power exceeds MFW flow by a predetermined limit. The feedwater control subsystem also includes a "Btu limiting" feature to limit the MFW demand signal so that the the final steam temperature is maintained. The primary output of the feedwater control subsystem is control signals to the MFW flow control valves (both startup and main) for each OTSG. Another output controls the MFW pump speed in order to maintain a specified pressure drop across the flow control valves as the MFW flow changes. Another output modulates the auxiliary feedwater (AFW) (ICS) flow control valves.



The reactor control subsystem matches the actual reactor power to the power demand signal from the integrated master subsystem, while maintaining  $T_{\text{ave}}$  at a constant value. The reactor control subsystem accomplishes this by sending signals to withdraw or insert the reactor control rods when the neutron power is outside a "deadband" around the neutron power demand.

The ICS is closely coordinated with the non-nuclear instrumentation (NNI) system since the purpose of a control system is to adjust the actual value of a process variable to a desired (i.e. demand) value. The NNI provides the input signals to the ICS that represent the actual values of numerous plant variables. When the signals representing plant variables are accurate and the ICS is functioning properly, plant control is smooth. If the NNI signals are not accurate, the ICS cannot sense the discrepancies and will initiate control actions based upon the erroneously indicated conditions. The resulting ICS control actions will not be appropriate and as a result a transient may be introduced throughout the plant that can be severe.

Many of the indicators in the control room (both meters and recorders) are nonsafety-related output devices and are in many cases part of the NNI system; hence, they are generally independent of the ICS. However, there are exceptions that had not been recognized by the plant operators at Rancho Seco prior to the December 26, 1985 incident. For example, the MFW flow recorders are affected by the ICS. During the December 26, 1985 incident, the recorder indicated a value near mid-scale due to the loss of ICS dc power, when MFW flow was actually zero.

### 3.1.3 Output Signals

The electrical output signals of the ICS at Rancho Seco take various forms. Throughout the internal modules of the ICS, a standard signal is used that varies between -10 Vdc and +10 Vdc. For control valves throughout the plant the ICS output signal reflects this standard signal (where -10 Vdc corresponds to fully closed, zero Vdc corresponds to a 50 percent open position, and +10 Vdc corresponds to fully open). This format was adopted because the ICS designers believed that the 50-percent position, which would be demanded upon loss of ICS power, would result in a transient of less magnitude than either a fully closed or a fully open demand signal. At Rancho Seco, the principal valves that are controlled by the standard +/-10 Vdc signal are the turbine bypass valves (TBVs), atmospheric dump valves (ADVs), MFW flow control valves (both startup and main), and AFW (ICS) flow control valves.

In addition, the ICS output signal to the turbine throttle valves (via the electro-hydraulic control) is in the form of pulses. Positive pulses cause the valves to open; negative pulses cause the valves to close; and zero output causes no motion.

The ICS output signal for the MFW pump speed varies from zero to +10 Vdc. A signal of 3.4 Volts or less corresponds to minimum speed and 7.3 Vdc or greater corresponds to maximum speed.

The ICS output signal for the reactor control rods is either +5 Vdc, zero, or -5 Vdc. The positive voltage corresponds to rod withdrawal; the negative voltage corresponds to rod insertion; and zero Vdc corresponds to no motion.

### 3.1.4 Loss of ICS dc Power

Upon loss of dc power within the ICS, there are three results. First, the various control modules lose power; hence, their outputs go to zero Vdc. Second, many switching relays lose power and go to the de-energized state. Third, manual control from the control room of ICS-controlled plant equipment is lost.

In summary, due to the zero Vdc outputs, the ICS will cause the following automatic actions: TBVs and ADVs go to the 50 percent stroke position; turbine throttle valves remain "as is"; main and startup MFW flow control valves go to the 50 percent stroke position; speed of the MFW pumps goes to minimum; AFW (ICS) flow control valves go to the 50 percent stroke position; and the reactor control rods remain "as is." It should be noted that the setpoint for the "MFW pump discharge pressure low" has been selected such that when the the MFW pumps are at minimum speed, the pressure switches trip and AFW is initiated automatically.

Upon loss of dc power, many ICS switching relays change state. One example is the relay associated with the operation of the stop valve for the main MFW flow control valve. The de-energized state corresponds to the startup MFW flow control valve being open less than 20 percent. When this condition exists, or the relay is de-energized by a loss of ICS power, the MFW stop valve is closed, thus automatically isolating flow through the main MFW flow control valve (but not the flow through the startup MFW flow control valve).

At Rancho Seco, when loss of ICS dc power occurs and devices change position automatically, operators in the control room lose remote control of ICS-controlled plant equipment. As a result, plant personnel must go to a variety of locations throughout the plant to operate ICS-controlled equipment manually (locally), a procedure that proved to be both time consuming and difficult to accomplish.

### 3.1.5 Restoration of ICS dc Power

Upon restoration of ICS dc power, the hand/auto control stations regain power in the "hand" mode (i.e., remote control from the control room is restored). However, it appears that the associated analog memory modules, which provide the actual control signal when in the "hand" mode; may reinitialize to one of the two full-scale demand positions. The ICS technical manual states that the reinitialized demand can be either zero percent or 100-percent demand, depending upon an internal connection within each memory module. The reactor operators reported that during the December 26, 1985 incident, the demand signal for several control valves was observed to be at 100-percent demand. No information on other types of demand signals upon restoration of power was reported. (The actual performances at Rancho Seco during a power restoration test is discussed in section 5.1.)

The effects of the restoration of ICS dc power are not well known. Further, the repeatability of ICS performance upon restoration of power is not fully understood, especially because the performance may depend upon the duration of the interruption of power. B&W has stated that the performance may also depend upon whether the + or the - 24 Vdc returns first. However, it is important to note that when ICS dc power is restored, reactor operators do regain remote control of plant equipment from the control room. During the December 26, 1985

incident, when ICS power was restored, the operators quickly readjusted the remote (CR) demand signals and were thereby able to terminate flow of AFW and stabilize plant conditions.

### 3.1.6 ICS Power Supplies and Distribution System

The ICS receives only 120 Vac power, and at Rancho Seco, two redundant 120 Vac buses provide this power. The first is a Class 1E vital instrumentation bus (i.e., bus 1C). The second is a non-Class 1E non-vital instrumentation bus (i.e., bus 1J). Both instrumentation buses are energized by inverters that are automatically powered by batteries upon loss of ac power. During the December 26, 1985 incident, vital bus 1C was energized by its normal inverter and non-vital 1J bus was energized by its alternate source, non-vital bus 1F. These 120 Vac instrumentation buses performed satisfactorily throughout the incident and played no role in the incident.

Internally the ICS needs both 120 Vac and +/-24 Vdc to operate its various components. The 120 Vac components include various field-mounted units such as electric-to-pneumatic converters plus contacts and relays that monitor certain plant conditions. The +/-24 Vdc, which is generated internally by the ICS, is needed to operate the numerous control modules of the ICS and various control switching relays.

As an example, Figure 3.3 illustrates the hardware of that small portion of the ICS that controls the turbine bypass valves for loop A. The purpose of the Figure 3.3 is to identify the different types of hardware involved and the type of power required to operate each type. Typical ICS modules are shown in Figure 3.6 which is a photograph of ICS cabinet no. 3. Figure 3.4 illustrates the typical ICS Hand/Auto control station and shows the meter that indicates the ICS demand valve.

Figure 3.5 depicts the power supplies and power distribution system within the ICS, starting with the 120 Vac supplied to the ICS. An automatic bus transfer (ABT) device is provided for the 120 Vac loads. The ABT is normally aligned to the vital bus, but will shift to the non-vital bus if power is lost from the vital bus and power is available from the non-vital bus. Automatic transfer of loads from the non-vital bus back to the vital bus is not allowed, in order to protect the vital bus from "load-side" faults. The 120 Vac loads of the ICS remained on the vital bus throughout the December 26, 1985 incident and had no role in the incident (i.e., the ABT did not transfer).

Power from each of the 120 Vac supplies to the ICS is used to operate pairs of 24 Vdc power supplies. Each ac supply operates one +24 Vdc power supply and one -24 Vdc power supply. Each power supply includes its own internal overcurrent and overvoltage protection circuitry. The outputs of these four power supplies are auctioneered to energize the +24 Vdc bus and the -24 Vdc bus within the ICS. Figure 3.6 is a photograph of ICS cabinet no. 3, showing the +/- 24 Vdc buses. If the output of any power supply should fall below the output voltage of its redundant power supply, the redundant power supply will provide the needed power via the auctioneering diodes. Similarly, if either one of the sources of 120 Vac to these dc power supplies is lost, the redundant configuration will provide the +/-24 Vdc power necessary to energize the buses and operate the ICS.

The +/-24 Vdc power system within the ICS also includes a power supply monitor module. This module monitors both the output voltage of each power supply and the voltage on the +24 Vdc bus and on the -24 Vdc bus. If any power supply output falls below a predetermined level (i.e., 23.5 Vdc), an annunciator alarm is activated in the control room. This alarm output is a "trouble alarm" (i.e., there is no immediate action required, but a loss of redundancy has occurred and a maintenance request should be initiated).

When the power supply monitor detects low voltage on either the +24 Vdc bus or the -24 Vdc bus (22.0 Vdc or less) or operates spuriously, it actuates the same annunciator alarm in the control room (i.e., the alarm for power supply trouble, described above, and for loss of a 24 Vdc bus, appears in the same annunciator window, i.e., "ICS or Fan Power Failure"). Further, this annunciator also is activated by a third input signal: loss of ICS cabinet ventilation flow. This "trouble alarm" does not require immediate action.

The action taken by the power supply monitor is to interrupt the incoming 120 Vac power to all four dc power supplies by sending a trip signal to the switches S1 and S2. These switches include integral nonadjustable time delays such that the switches will trip to the OFF position if the bus voltage does not recover within 0.5 seconds. Figure 3.7 is a photograph of switches S1 and S2. The ICS will function properly when the voltages are maintained within +/-10 percent of 24 dc. The rationale for opening these switches is that, if the voltage falls outside this range, the performance of the ICS is undefined. Moreover, the performance is not fully predictable and may be inappropriate. Therefore, any degraded voltage situation is an "unknown" failure mode. Thus, the system is designed to automatically transform any degraded voltage situation into a complete loss of power situation. This latter failure mode was thought to be better understood.

The incoming power switches S1 and S2 are operated by only two mechanisms: manually by an operator, and automatically by the power supply monitor. Since there is only one power supply monitor, it is an obvious potential single failure point.

On December 26, 1985, the ICS suffered a complete loss of its dc power and the switches S1 and S2 were later found in the OFF position. This loss of ICS dc power was the transient initiator.

### 3.2 Auxiliary Feedwater System

The auxiliary feedwater (AFW) system, Figure 3.8 is designed to provide an adequate water supply to the once-through steam generators (OTSGs) for reactor decay heat removal during periods when the main feedwater (MFW) supply is unavailable or when electrical power to all four reactor coolant pumps (RCPs) is lost. The AFW system actuates automatically on loss of both MFW pumps (at a discharge pressure of less than 850 psig), loss of all four RCPs, or upon receipt of a safety features actuation system (SFAS) signal (indicating a reactor coolant system pressure of less than 1600 psig or a reactor building pressure of greater than 4 psig).

The AFW system consists of a water supply source, two pumps, and associated piping, valves, and instrumentation. The normal water supply is from the

450,000-gallon condensate storage tank (CST). After depleting the CST, the pumps can be manually realigned to draw water from the plant reservoir.

Each of the AFW pumps is rated at 840 gallons per minute (gpm) when pumping at a discharge pressure of 1162 psig. Approximately 60 gpm is used for recirculation flow back to the main condenser. Thus, the net flow to the OTSGs would be 780 gpm. One AFW pump (P-318) is a dual-drive pump, being equipped with both a steam turbine and an electric motor mounted on the same shaft as the pump. The AFW pump turbine receives steam from either OTSG through the main steam header, and can also be supplied from the auxiliary steam header. The electric motor is powered from Class 1E 4160 Vac nuclear service bus 4B. AFW pump P-319 is driven by an electric motor only. It is powered from Class 1E 4160 Vac nuclear service bus 4A.

The dual-drive AFW pump is normally aligned to the A OTSG and the motor-driven AFW pump is normally aligned to the B OTSG. However, a cross-tie line is provided between the two AFW headers. The motor-operated cross-tie valves (HV-31827 and HV-31826) are provided (normally open) allowing either pump to supply either OTSG.

AFW flow can be either automatically or manually controlled using air-operated flow control valves FV-20527 and FV-20528. The position of these valves is controlled by the ICS. As discussed in Section 3.1, loss of dc power within the ICS causes these valves to assume the 50 percent stroke position. Manual handwheels are provided that enable the operator to operate the valves locally, if necessary.

In the case of loss of MFW or loss of all four RCPs, both AFW pumps automatically start (the dual-drive pump is steam powered). In the event of an SFAS initiation, the electrically driven pump (P-319) is shed from bus 4A and then sequentially loaded back on the bus, a process that takes approximately 30 seconds if the SFAS signal was not accompanied by a loss of bus voltage, and 40 seconds if there was a loss of bus voltage and the diesel generator is picking up essential loads. The dual-drive pump starts immediately and is steam-powered.

The AFW system includes separate flow control valves that are controlled by the safety features actuation system (SFAS). The valves (SFV-20577 and SFV-20578) are located in bypass lines around each ICS-controlled flow control valve. Upon receipt of an SFAS signal, the SFAS-controlled valves open fully to provide flow to the OTSGs. These valves can be opened or closed remotely from the safety features panel in the control room.

Throughout this report, the ICS-controlled flow control valve will be referred to as the "AFW (ICS) flow control valve" and the SFAS-controlled flow control valve will be referred to as the "AFW (SFAS) flow control valve."

Locked-open manual isolation valves (FWS-063 and FWS-064) are located downstream of the AFW flow control valves and safety feature valves. Shutting the manual isolation valve isolates flow from both the AFW (ICS) flow control valve and the AFW (SFAS) flow control valve to the respective OTSG. However, if a single isolation valve is shut and the cross-tie valves are open, much of the flow will be diverted to the other OTSG.

### 3.3 Main Feedwater System

The main feedwater (MFW) system, Figure 3.9, consists of two 80-percent capacity turbine-driven feedwater pumps and the associated piping, valves, and instrumentation necessary to provide feedwater to the OTSGs.

The pumps take a suction from the low pressure feedwater heater trains and discharge through two parallel high pressure feedwater heater trains. Feedwater is then directed to a common supply header, thereby allowing a single MFW pump to feed both OTSGs at low power. The supply header branches into two supply lines, one connected to each OTSG. Each supply line contains a 16-inch main MFW flow control valve (FV-20525 and FV-20526) and a MFW stop valve (FV-20529 and FV-20530). Two 6-inch startup MFW flow control valves (FV-205075 and FV-20576) are provided that bypass both the main MFW flow control and the MFW stop valves.

The two MFW pumps (P-317A and P-317B) are turbine-driven, double suction, single stage, centrifugal pumps. Each pump is rated at 15,600 gpm and is capable of supplying both OTSGs with approximately 80 percent capacity against full secondary pressure. Minimum recirculation flow of 1600 gpm is directed to the low pressure condenser. Steam from the moisture separator reheaters is used when plant load is 40 percent or greater. High pressure steam from the main steam system supplements the low pressure steam at higher plant loads. Any steam used to drive the turbines is exhausted to the low pressure section of the main condenser. Steam to the turbines is provided from the auxiliary steam system, which receives steam from an auxiliary boiler during plant startup and low power operations.

The MFW pumps are initially started from the startup pushbutton station in the control room. After MFW pump turbine speed automatically increases to approximately 3000 rpm controls are transferred to the hand/auto station in the control room. At this point, control is either remote (CR) or automatic. In automatic, the ICS controls the MFW pump turbine. (See Section 3.1 for a detailed discussion of the ICS.) Upon loss of ICS dc power, MFW pump turbine speed is run back to the minimum speed of approximately 2500 rpm. At this speed, the pumps will not pump against any significant OTSG pressure.

The main MFW flow control valves (FV-20525 and FV-20526) are cylinder-operated, air-to-open/spring-to-close, angle globe valves. They are capable of passing  $6.12 \times 10^6$  lbm/hr of feedwater at operating pressure of 1050 psig and temperature of 470°F. Pressure drop across the valves is controlled at 35 psid by varying the pump speed. The startup MFW flow control valves (FV-20575 and FV-20576) are cylinder-operated, air-to-open/spring-to-close, gate valves. They are capable of passing 820,000 lbm/hr of feedwater and have a normal pressure drop of 35 psid. The startup MFW flow control valves are used to control feedwater flow during startup, shutdown, and low power operations. The positions of the main MFW flow control valves and startup MFW flow control valves are normally controlled automatically by the ICS. The valves are also capable of being operated remotely from the control room. As discussed in Section 3.1, loss of dc power within the ICS causes the main MFW flow control valves and the startup MFW flow control valves to assume a 50-percent stroke position, and causes a loss of remote control from the control room.

The motor-operated MFW stop valves (FV-20529 and FV-20530) are located immediately downstream of the main MFW flow control valves. The MFW stop valves are interlocked (through the ICS) to open automatically when the startup MFW flow control valves are opened to 80 percent or greater. Likewise, the MFW stop valves automatically close when the startup MFW flow control valves are open 20 percent or less. Control relays for these interlocks are part of the ICS. The de-energized state for these relays corresponds to the startup MFW flow control valve being closed. Thus, loss of ICS dc power causes the MFW stop valves to automatically close.

The main steamline failure logic (MSFL), a non-class 1E system, causes automatic closure of the main and startup MFW flow control valves on indication of a steam line rupture. By isolating feedwater to the affected OTSG, it is allowed to steam dry (i.e., empty), thereby removing it as a heat sink from the reactor. This action helps to minimize the cooldown rate, which could be excessive in the event of a steam line rupture. The valves close automatically when their respective main steam header pressure drops below 435 psig. After the MSFL logic closes the main and startup MFW flow control valves, the ICS closes the motor-operated MFW stop valves. (Section 9.1 provides additional information regarding the MSFL.)

### 3.4 Once-Through Steam Generators

Reactor coolant water enters the top of the OTSGs and flows down through the vertical tubes giving up its heat to the secondary side fluid in the process. It then passes out the lower head where it is directed back to the reactor (see Figure 3.10).

MFW is supplied to the OTSG from an external ring header through nozzles spaced equally around the periphery of the OTSG. Incoming feedwater mixes with aspirating steam which preheats the main feedwater, flows down through the downcomer region, and through the water ports into the tube bundle at the lower tubesheet. The water then begins to boil and the water/steam mixture flows upward through the shell side of the tube bundle. When the steam reaches the top of the tube bundle, it is directed into the steam annulus, and then out through the steam nozzles.

AFW is supplied through a circular header located within the upper part of the steam annulus. The header contains holes that spray AFW directly onto the tubes in the upper portion of the tube bundle. The AFW header is located high in the OTSG to ensure that the relatively cold AFW (approximately 70°F) is sufficiently heated before reaching the lower shell and tubesheet to avoid thermal stresses. This feature also provides for a considerable transfer of heat from the RCS to the feedwater, even when the water level is quite low in the OTSG.

Several instruments that detect water level are provided on each OTSG (see Figure 3.10) as follows:

1. Startup range instruments measure from 0 to 250 inches. The "0 inch" level corresponds to approximately 16 inches above the lower tubesheet. The startup range instruments are calibrated "hot" but are not temperature compensated. Indication is provided in the control room and on the safety parameter display system (SPDS) screen. The OTSG low water

level alarm (which has a setpoint of 24 inches) comes off the startup range instrument.

2. Operating range instruments measure from 0 to 100 percent. Several readings can be correlated to levels above the tubesheet.
  - 10% = 24 inches
  - 50% = 135 inches
  - 96% = 384 inches (just below the steam aspirating ports)

The operating range instruments are temperature compensated and provide input to the control room indicators, the SPDS screen, and to a strip chart recorder. A high level alarm (82.5 percent) is controlled by the level recorder, and provides input to the control room annunciator.

3. Full range instruments measure from 0 to 600 inches. The transmitters are calibrated "cold" and are not temperature compensated. Indication is provided in the control room, and also on the remote shutdown panel (in the west nuclear service bus room) and the boron analyzer panel (in the computer room immediately adjacent to the control room). Transmitters for the latter two indicators are powered from 24 Vdc vital power (this is a separate power source that is not associated with the 24 Vdc ICS power supply).

### 3.5 Main Steam System

The main steam system distributes steam from the two OTSGs to the high pressure turbine, the two turbine-driven MFW pumps, the dual-drive AFW pump, and to other miscellaneous loads (see Figure 3.11).

Superheated main steam at 925 psig leaves each OTSG through two 24-inch steam lines that combine into one 36-inch line inside the containment building. Main steam then flows through the 36-inch headers through turbine throttle valves and turbine control valves to the high pressure turbine. Rancho Seco does not have main steam isolation valves (MSIVs). There are several taps off the main steam headers between the OTSGs and the turbine throttle valves; the principal ones are described in the following paragraphs.

Each OTSG and its associated main steam piping is protected from overpressure by nine ASME code safety valves. The nine valves are grouped into four sets of valves, with graduated set points from 1050 psig to 1102.5 psig. Steam is released from the safety valves and directed to the atmosphere through individual 18-inch diameter stacks. The total design capacity of the safety valves is approximately 120 percent of system design steam flow, which allows the energy generated at the reactor high power trip set point to be dissipated, even with one safety valve inoperable.

In addition, turbine bypass valves (TBVs) and atmospheric dump valves (ADVs) are provided to accept excess steam from the system. The TBVs and ADVs, combined with control rod motion, are designed to accommodate up to a 50-percent step decrease in turbine load without actuating the code safety valves. The TBVs and ADVs are also used during plant heat-up and cooldown.



There are four TBVs, two on each main steam header. Steam passes through the TBVs and is discharged into the high pressure section of the main condenser through perforated spray pipes. The total capacity of the four TBVs is 15 percent of full load steam flow. Each TBV is an air-operated 8-inch globe valve.

The positions of the TBVs are set by a pneumatic positioner that is operated by air from an electric-to-pneumatic converter which is controlled by the ICS. The TBVs are normally controlled automatically, or remotely from the control room hand station. Both of these modes are dependent upon ICS power. They are also capable of being operated from the remote shutdown panel outside the control room, independent of ICS power. They may also be operated locally, using handwheels mounted on each valve. The valves can also be isolated by shutting manual valves upstream of the TBVs.

There are six ADVs, three on each main steam header. As the name implies, steam passes through each ADV and is discharged through 14-inch diameter stacks to the atmosphere. The ADVs are identical in construction to the TBVs. The combined capacity of the six ADVs is 25 percent of full load steam flow. To preclude excessive cooldown on inadvertent opening of the ADVs, four of the six ADVs are normally isolated using local handwheels. (Note that in this configuration, the probability of the code safety valves lifting is increased following a large decrease in turbine load.) The ADVs are controlled automatically by the ICS or remotely by the control room hand station, the same as the TBVs. They are also capable of being operated from the remote shutdown panel or from an ADV manual control panel outside the control room. Both of these panels function independently of ICS power.

The TBVs and ADVs fail closed on loss of air pressure, and fail to the 50-percent open position on loss of ICS dc electrical power.

Main steam is also supplied to operate the MFW pump turbines through valves HV-20565 and HV-20560. One of these valves is normally open while the other is closed. The main feedwater system is described in Section 3.3.

Steam to the dual-drive AFW pump turbine taps off the lines to the TBVs, passing through check valves and normally open motor-operated valves (HV-20569 and HV-20596) to the normally closed steam inlet control valve (SFV-30801). The AFW system is described in Section 3.2.

Other taps off the main steam header include lines to the moisture separator reheaters and lines supplying "pegging" steam to the second and fourth point feedwater heaters. The normal source of feedwater heating is from turbine extraction steam. As turbine load is reduced, "pegging" steam from the main steam header is supplied to the feedwater heaters to augment turbine extraction steam. Motor-operated isolation valves for these lines are controlled from handstations in the control room.

### 3.6 Makeup/High Pressure Injection System

The makeup system is used to maintain RCS coolant inventory and to provide cooling and lubrication to the reactor coolant pump (RCP) seals. This makeup function is normally accomplished by aligning the makeup pump (P-236) to take suction from the makeup tank (MUT) and discharge to the RCP seals and to the RCS through a high pressure injection (HPI) nozzle. (See Figure 3.12.) The

makeup system shares common sources of water and piping with the HPI portion of the emergency core cooling system. Either of the HPI pumps (P-238A and P-238B) can be used as a backup to the makeup pump during normal plant operations, and the makeup pump can serve to supplement the HPI pumps during a safety features actuation.

The makeup pump and HPI pumps are identical horizontally mounted, nine-stage, centrifugal pumps. Each is rated for a normal discharge pressure of 2900 psig, with a flow rate of 300 gpm. A minimum net positive suction head (NPSH) of 30 feet is required to prevent the pumps from cavitating. An ac motor that turns at 1780 rpm is connected to each pump through a high speed gear drive, resulting in a pump speed of 6018 rpm.

These are multi-stage pumps, operating at high pressure, generating considerable internal heat due to frictional losses. A minimum flow of 105 gpm is needed through the pumps (through the minimum flow lines) during continuous operation to avoid the potential for pump damage. The minimum flow can be reduced to 40 gpm, but only if the pump is operated less than 15 minutes. The maximum allowable pump operating time when flow is less than 40 gpm is 15 seconds.

Water to the pumps can be supplied from either the MUT (capacity = 4500 gallons), or from the borated water storage tank (BWST) (capacity = 450,000 gallons). The MUT is the normal supply to the makeup pump (P-236), through a motor-operated suction valve from the MUT (SFV-23508) and a manual pump suction isolation valve (SIM-001). On a safety features actuation, the suction valve from the MUT closes to isolate the MUT while the supply valves from the BWST (SFV-25003 and SFV-25004) open. A relief valve on the outlet of the MUT relieves to the flash tank.

Between the suction valve from the MUT (SFV-23508) and the makeup pump suction isolation valve (SIM-001), a common cross-connect line is provided to supply water from the MUT to the two HPI pumps (P-238A and P-238B). There are four manual isolation valves in this common line; two between the makeup pump and each HPI pump. Normally the makeup pump (P-236) and the A HPI pump (P-238A) take suction from the MUT. Therefore, the associated cross-connect valves are open. The B HPI pump (P-238B) normally takes a suction from the BWST, so its cross-connect valves are closed.

The pumps discharge into a cross-connected header containing four normally open manual isolation valves. This arrangement allows any of the three pumps to supply normal makeup to the RCP seals and to the RCS. A minimum flow line taps off the discharge of each pump to allow sufficient flow for pump cooling. The minimum flow lines from all three pumps combine into a single header that directs the water to the upstream side of the seal return coolers and back to the MUT. The header contains two motor-operated valves (SFV-23645 and SFV-23646) that close on a safety features actuation to ensure full flow to the RCS.

During normal operations the makeup pump supplies the RCP seals through safety features valve SFV-23616. Normal makeup is provided through SFV-23604, and then through the A HPI line where the line connects to the RCS on the discharge side of the A RCP. On an SFAS initiation, SFV-23604 closes automatically to isolate normal makeup, and HPI safety features valves (SFV-23809, SFV-23810, SFV-23811, SFV-23812) open. On an SFAS initiation, the makeup pump supplements

the A and B HPI pumps (P-238A and P-238B) through the open pump discharge cross-connect lines.

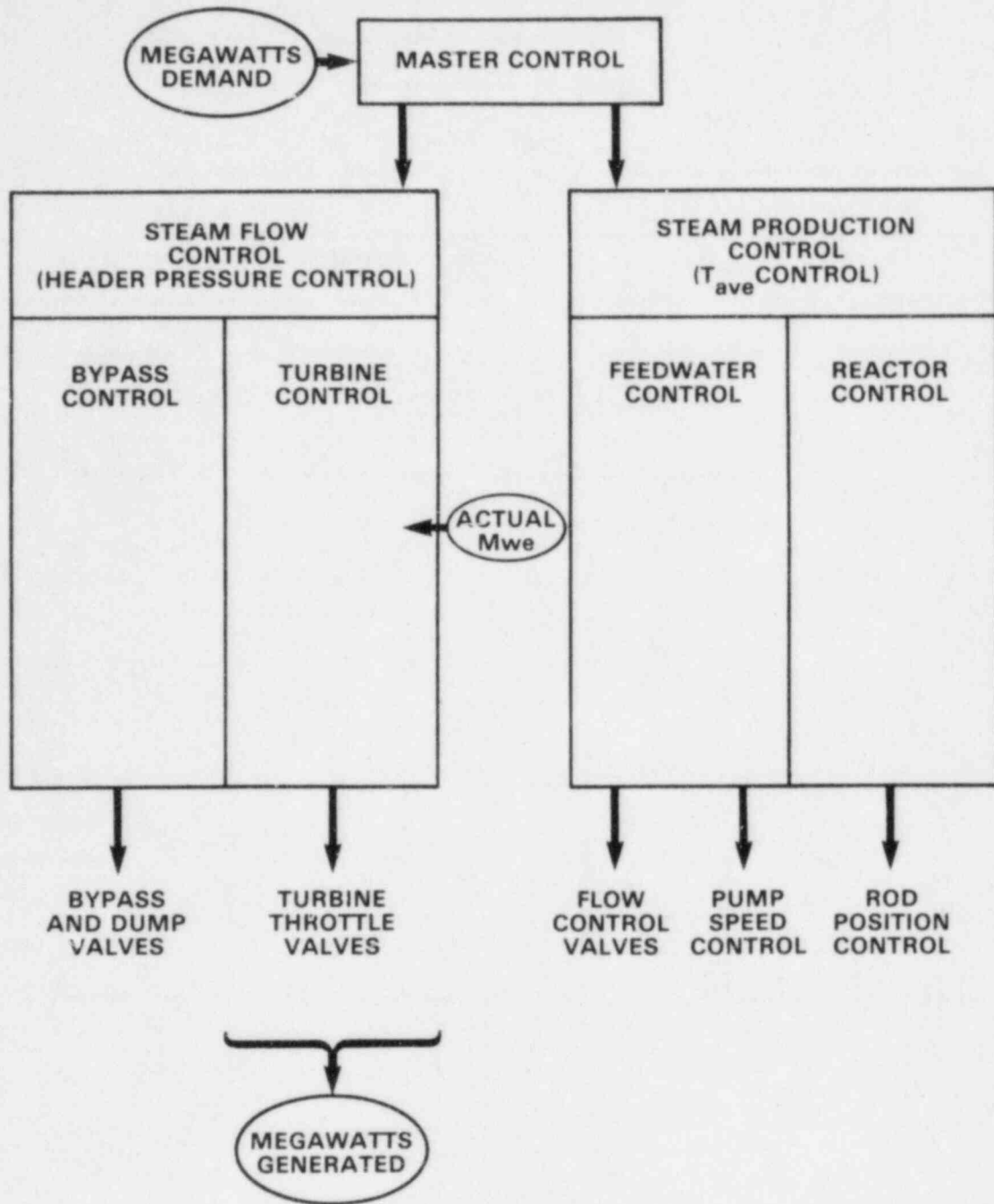


Figure 3.1 Rancho Seco basic plant control concept

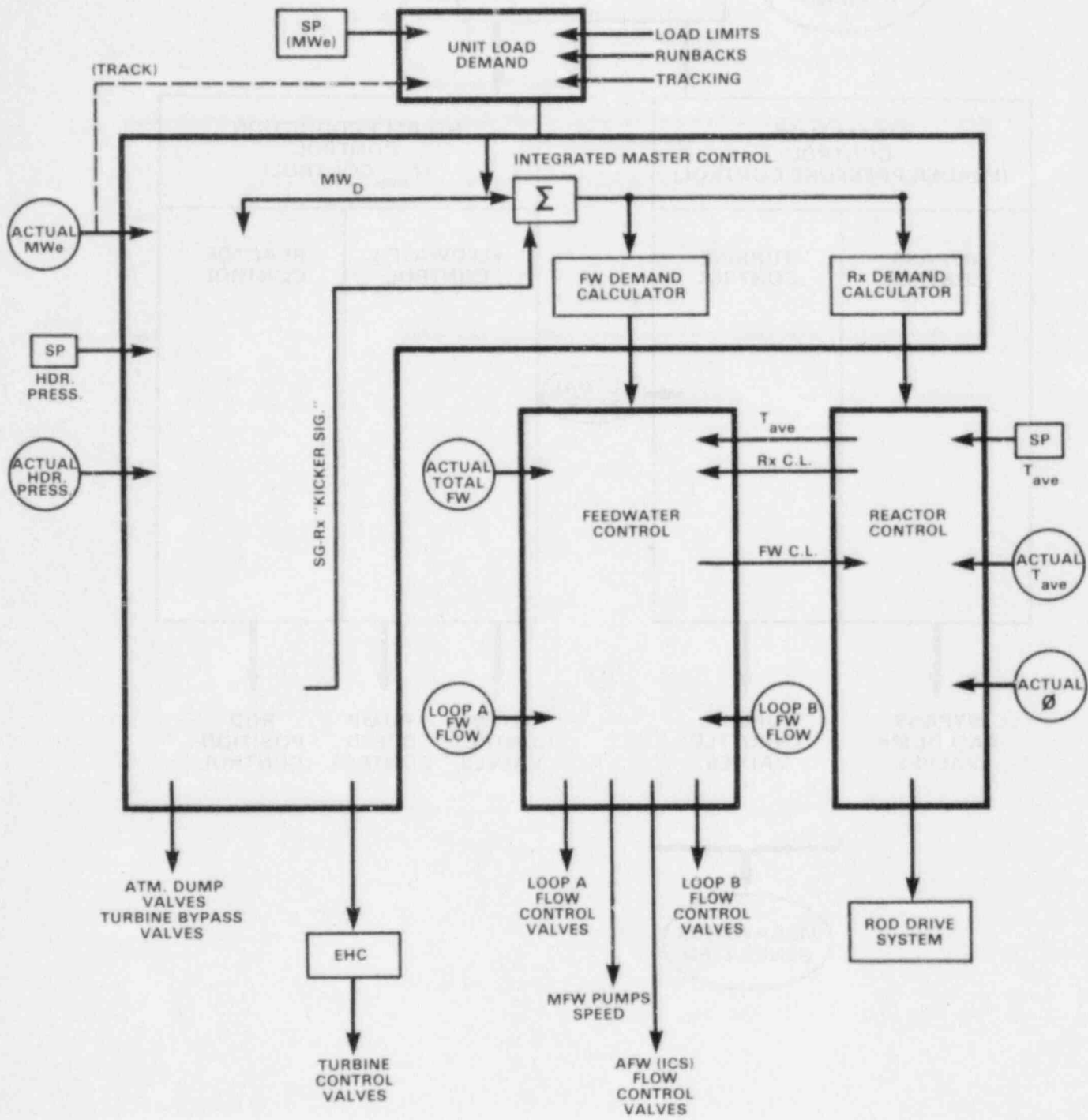


Figure 3.2 The Rancho Seco integrated control system

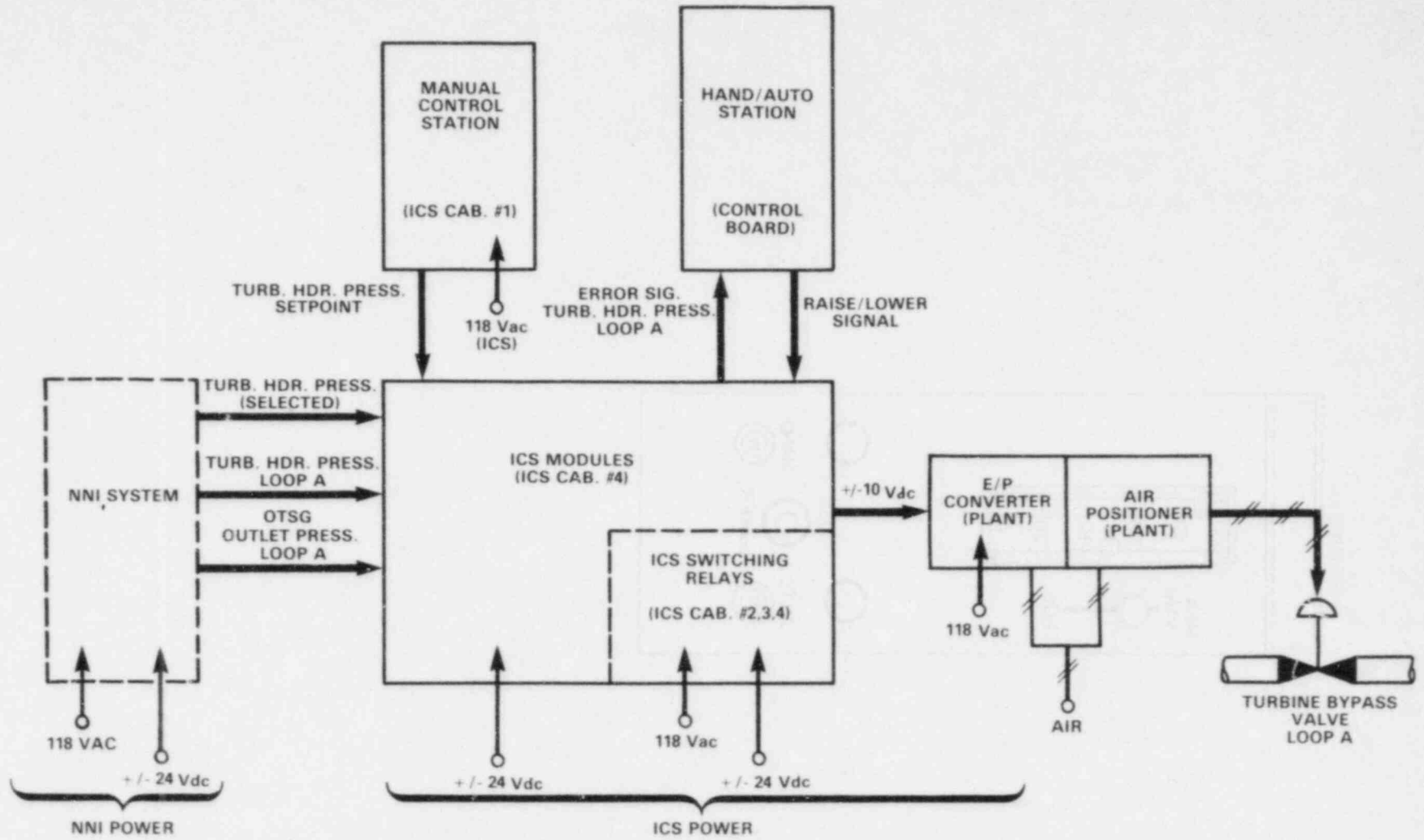


Figure 3.3 Equipment diagram--control of turbine bypass valve A

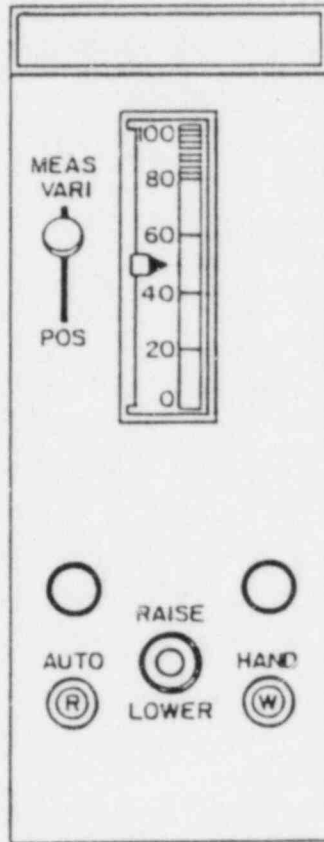


Figure 3.4 Typical ICS "hand/auto" control system

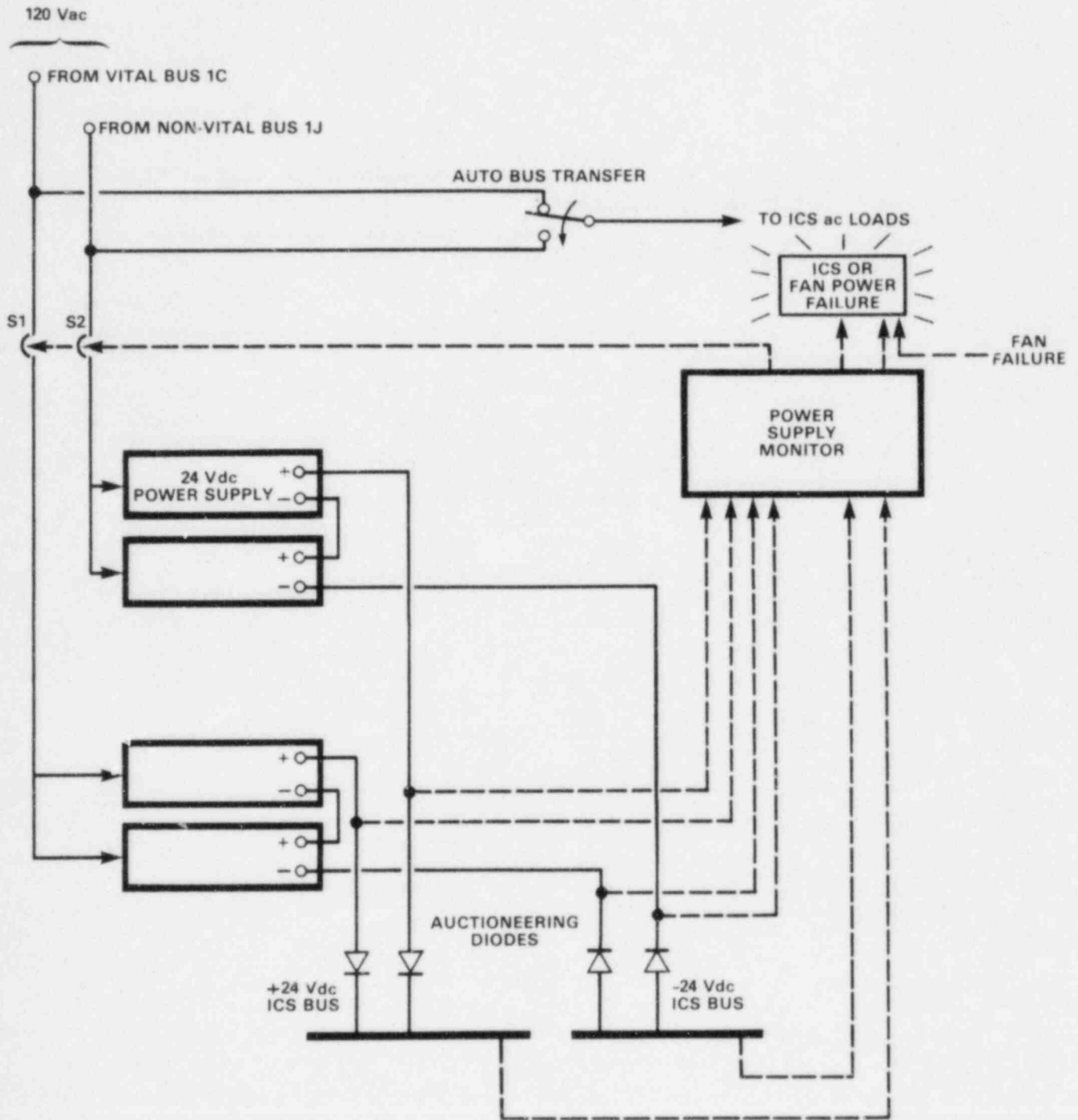
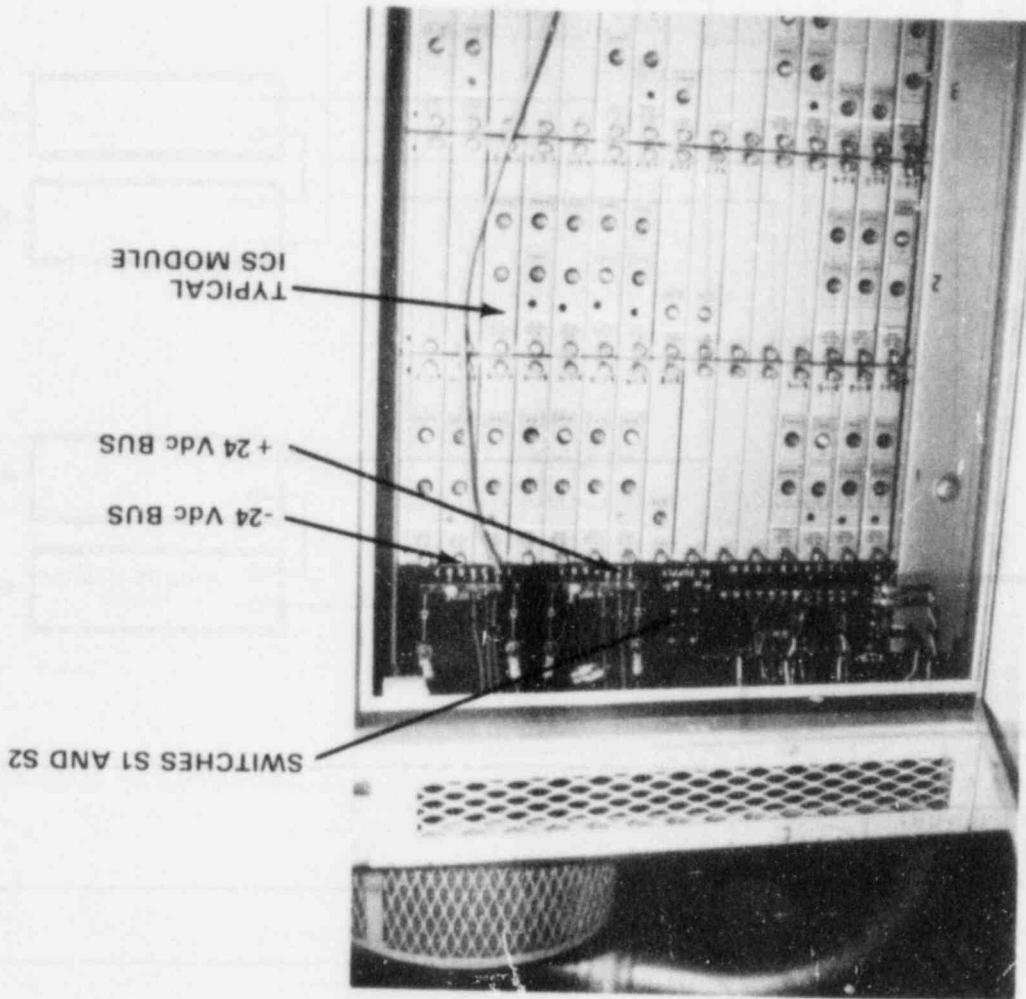


Figure 3.5 ICS direct current power supplies



Figure 3.6 ICS +/-24 Vdc buses (ICS cabinet no. 3)



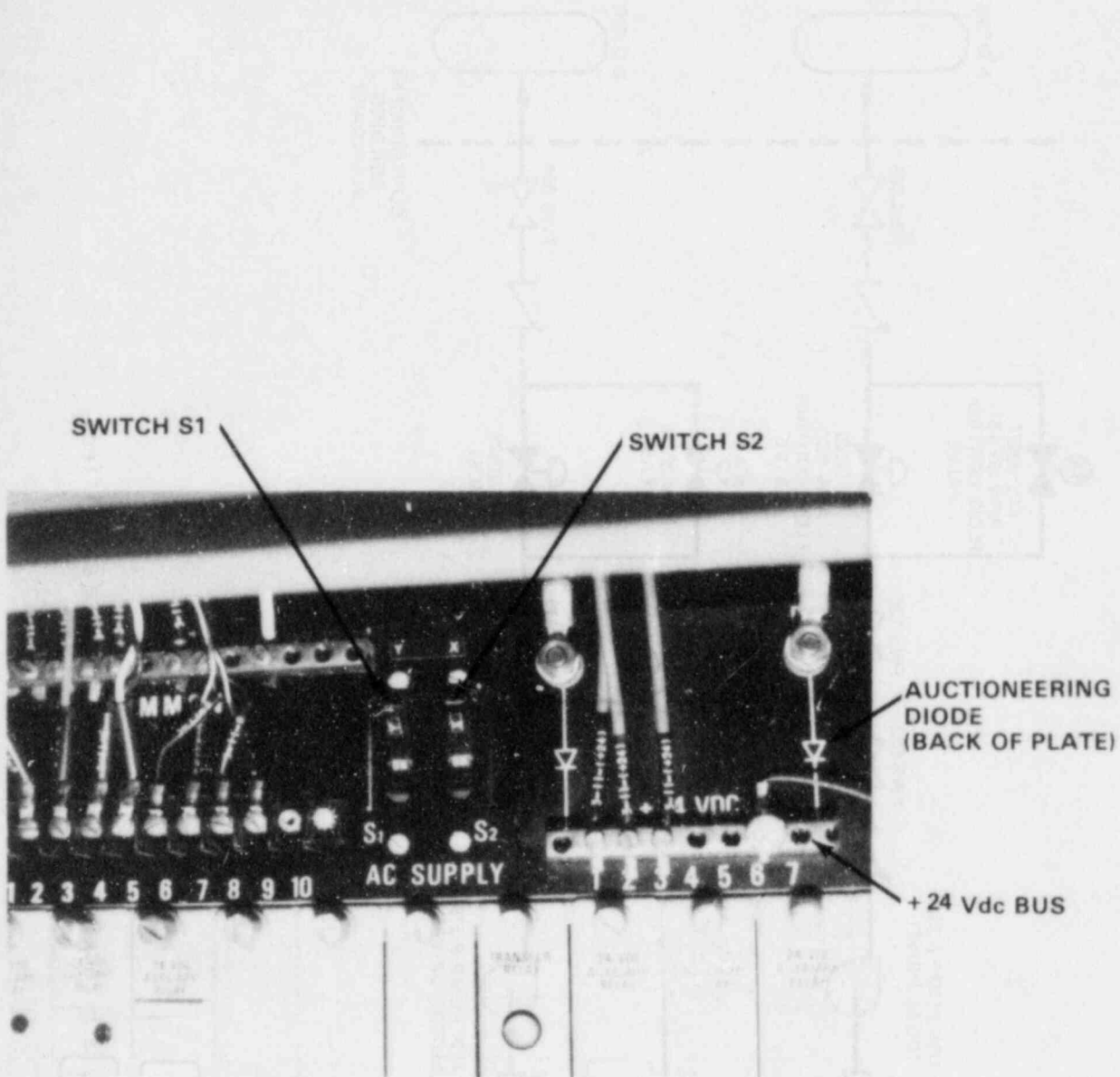


Figure 3.7 ICS power switches S1 and S2

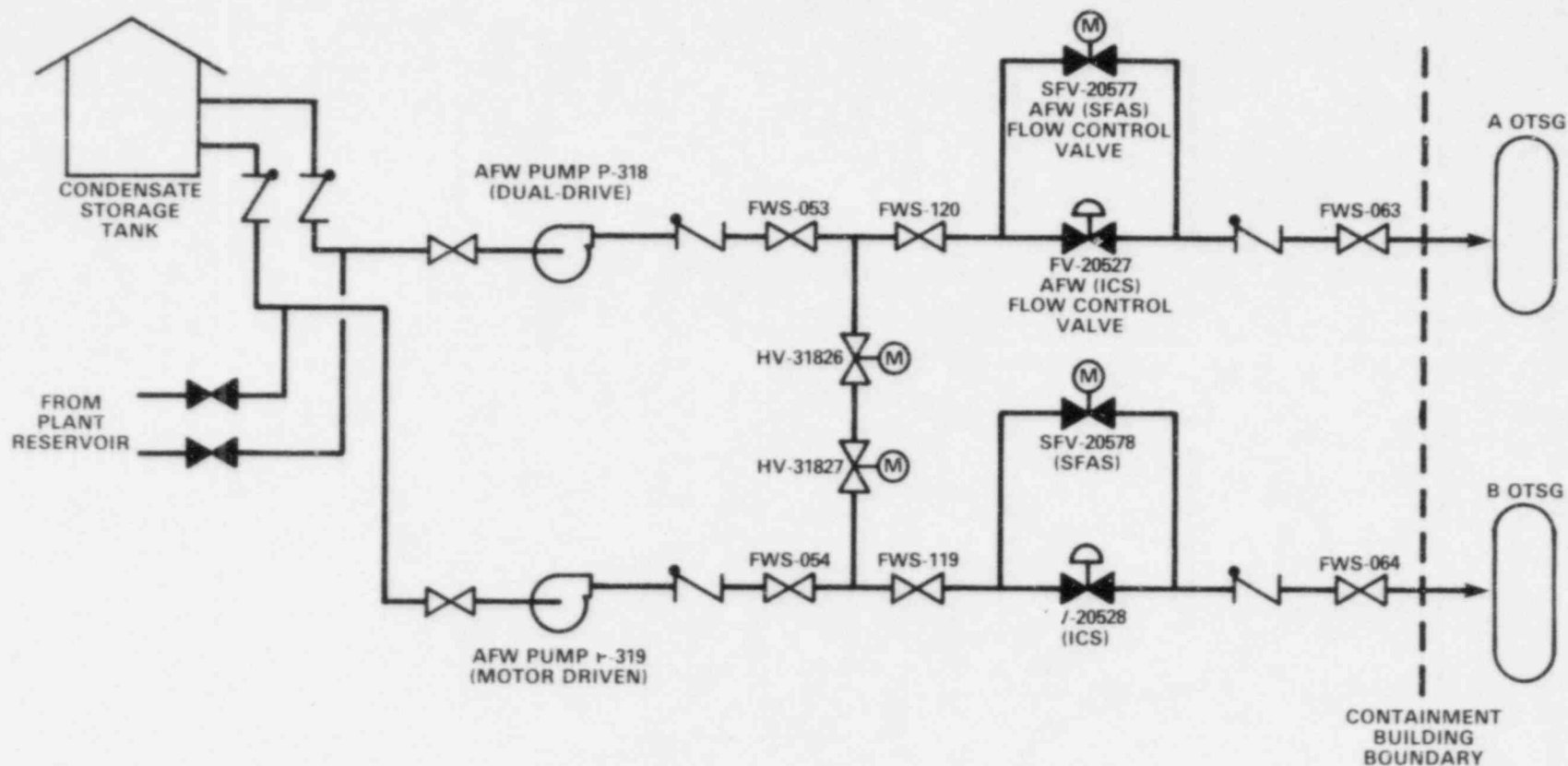


Figure 3.8 Auxiliary feedwater system (simplified)

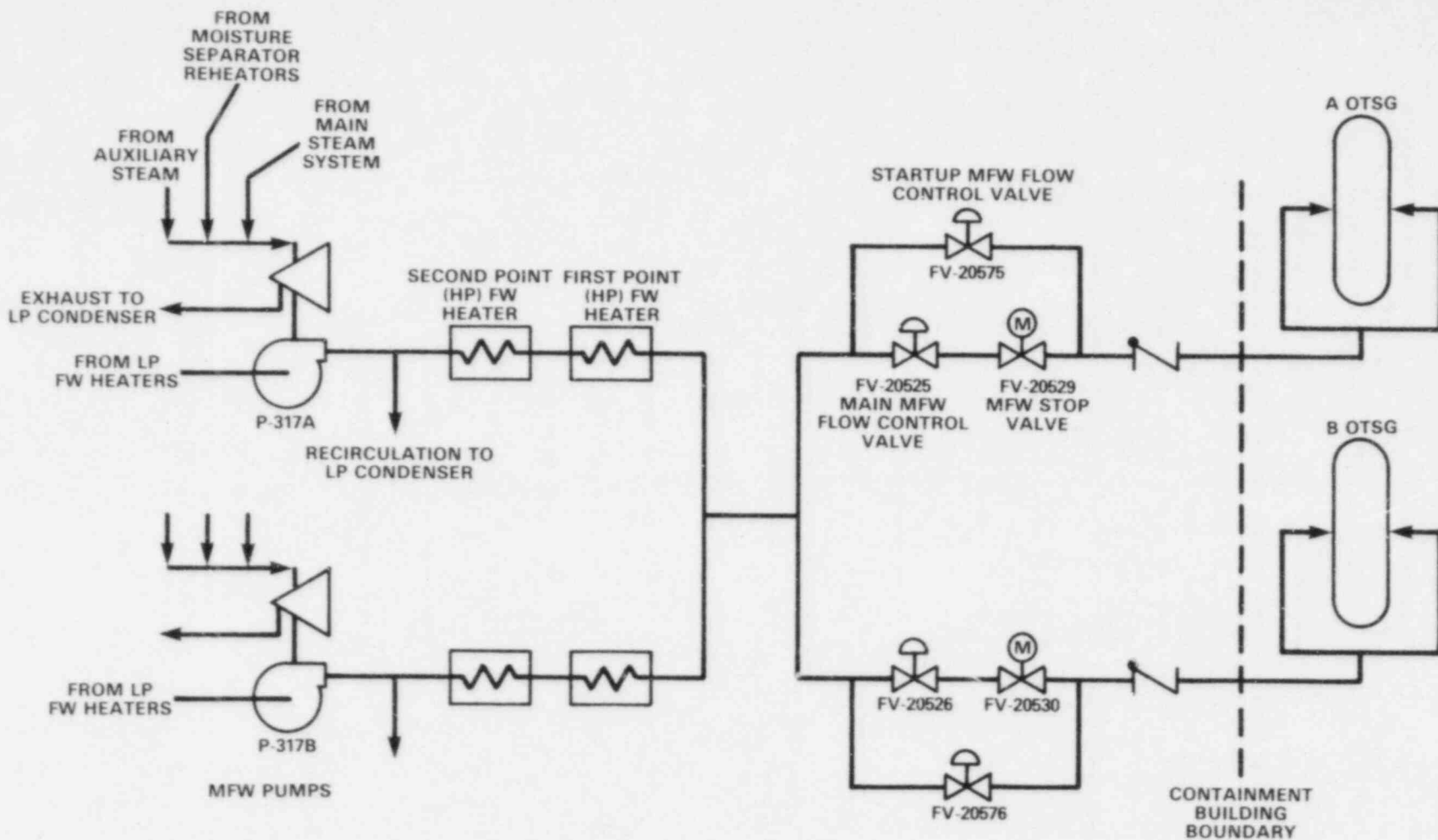


Figure 3.9 Main reedwater system (simplified)

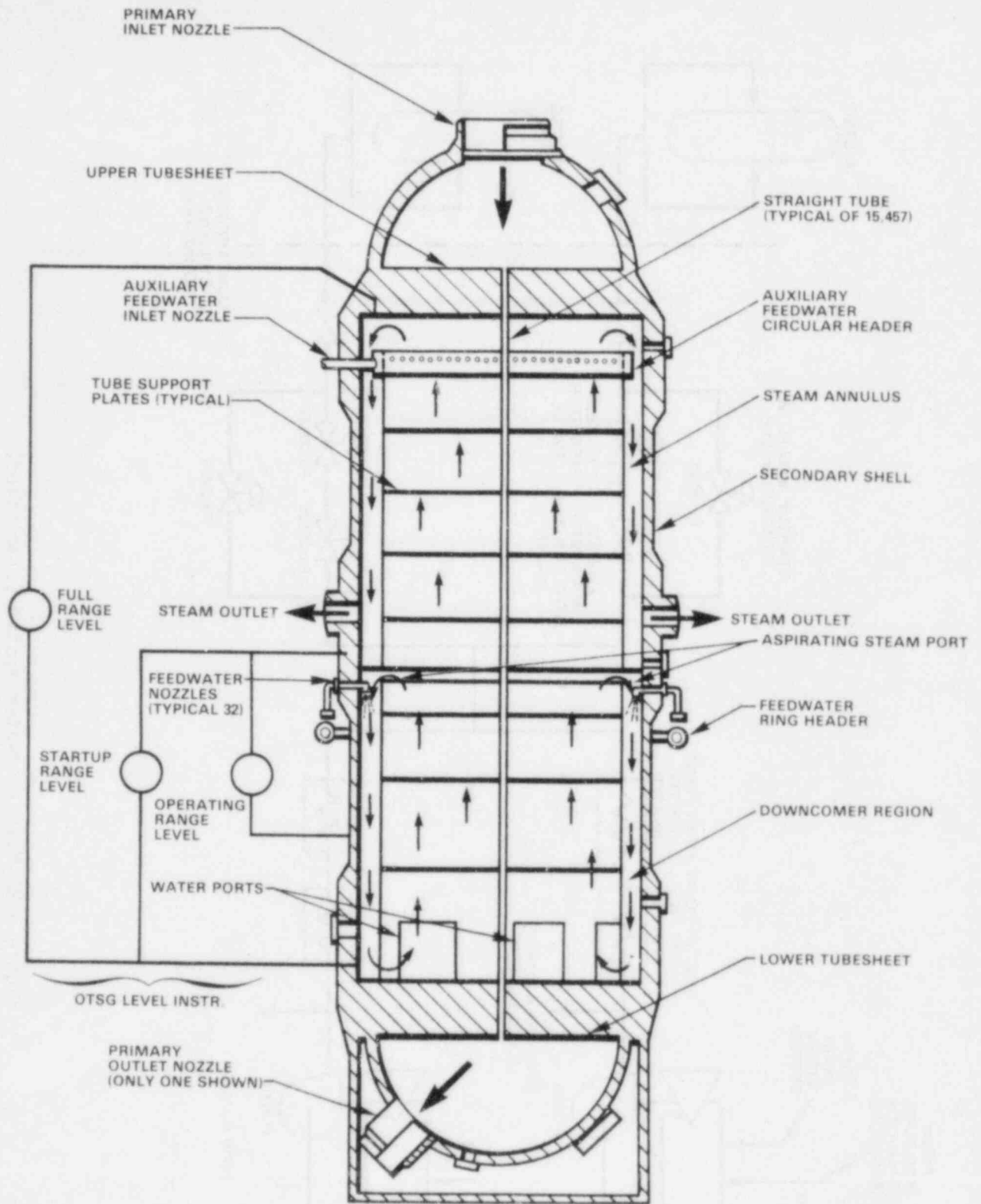


Figure 3.10 Once-through steam generator flow paths and level indicators

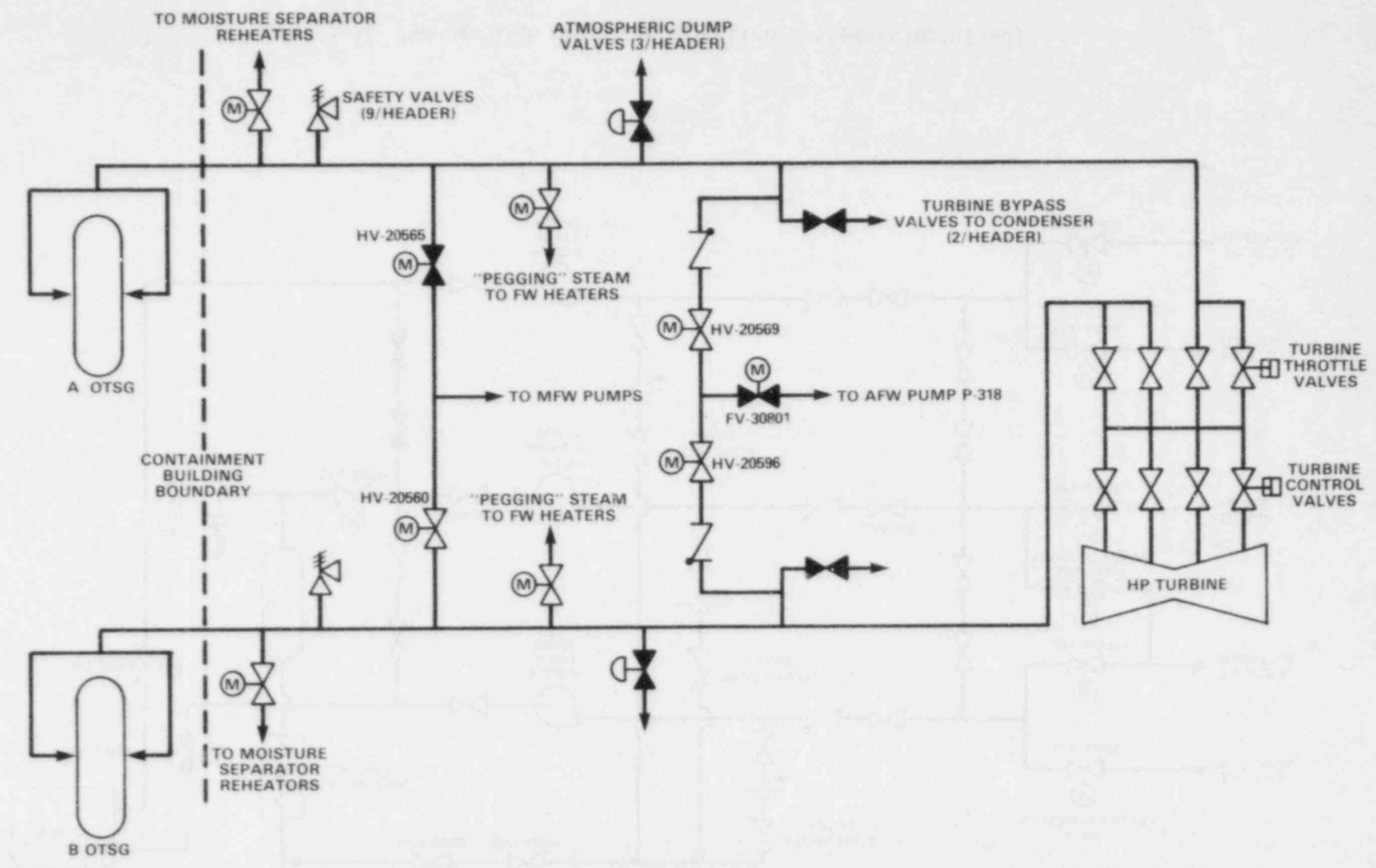


Figure 3.11 Main steam system (simplified)

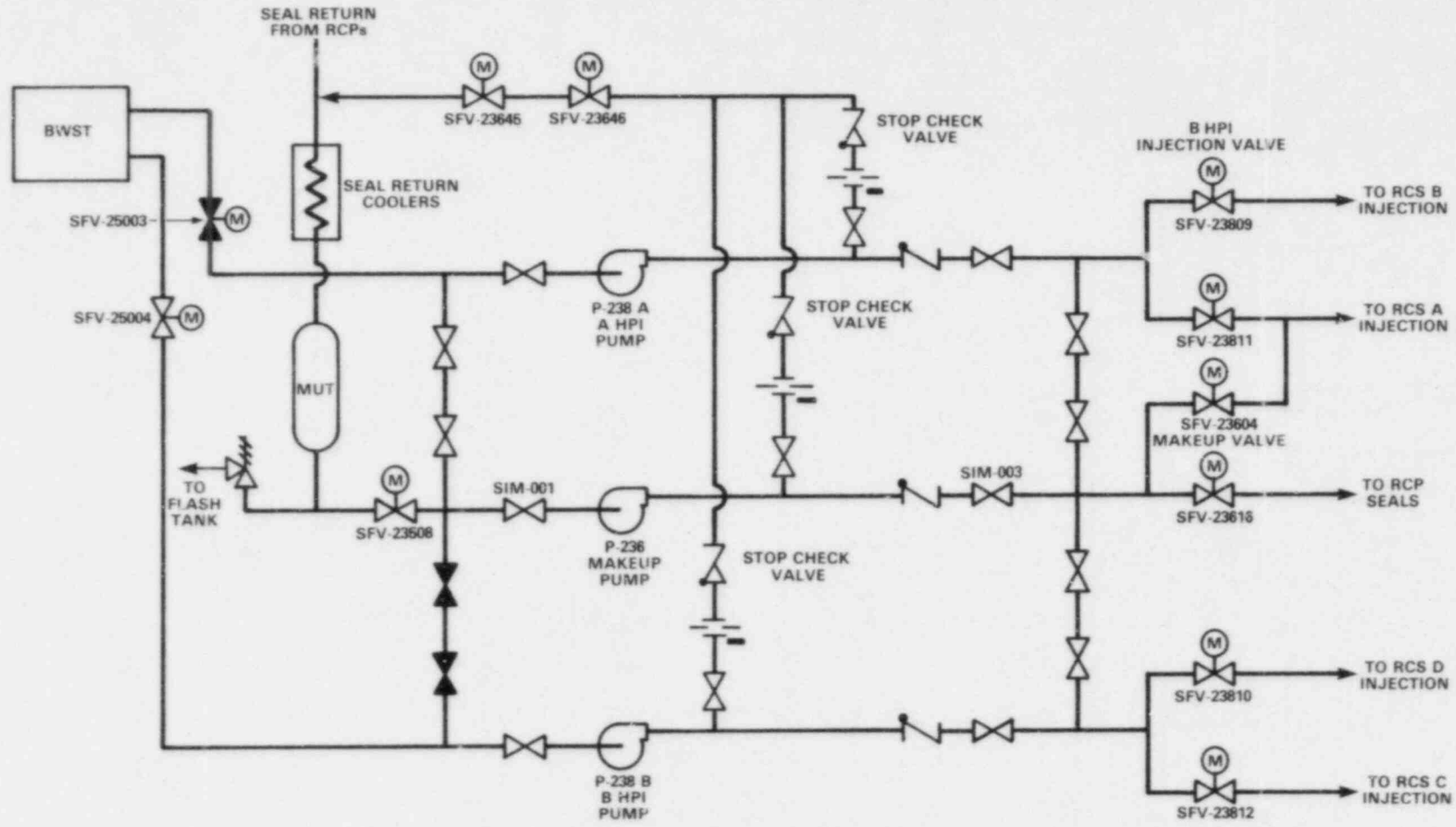


Figure 3.12 Makeup/high pressure injection system (simplified)

## 4 NARRATIVE OF THE INCIDENT

This section provides a narrative description and a sequence of events of the loss of dc power within the integrated control system (ICS) at Rancho Seco and subsequent overcooling and partial repressurization of the reactor coolant system (RCS). One of the two main plant computers (the Bailey) was out of service prior to this incident. A backup computer, the interim data acquisition and display system (IDADS), was available. Since the Bailey computer was out of service, its post-trip review and alarm printout and its normal input to the IDADS were not available. The NRC Incident Investigation Team (the Team) created this narrative and the chronological sequence of events listed in Table 4.1 from a composite of IDADS data, operator and management interviews, logs kept by reactor operators, and interpretations of strip charts from plant trend recorders. Figures 4.1 through 4.6 provide plots of various data recorded by the IDADS.

### 4.1 Plant Status and Oncoming Shift

On December 25, 1985 at 11:30 p.m., the midnight shift of operators reported for shift change. With the exception of the plant computer out of service, the plant was functioning normally. The plant had just resumed operation on December 24 following a two-day outage for valve repairs. The oncoming shift included four Senior Reactor Operators, one of whom was the Shift Technical Advisor (STA); two Reactor Operators; and six Nonlicensed Operators. Three of the Nonlicensed Operators were Auxiliary Operator Trainees and all were qualified as either Equipment Operators and/or Power Plant Helpers; they functioned in those positions during the incident. (For a detailed listing of those on duty, see Section 6.2.) Although the 12 employees on shift made up less than the normal shift complement, they constituted 5 more than the 7 operators required by the plant Technical Specifications or the Sacramento Municipal Utility District (SMUD) commitments.

The plant had gradually increased power to 76 percent (712 Mwe) of full licensed power, then stabilized. Reactor decay heat was, therefore, relatively low, a condition that would later exacerbate the overcooling transient. Reactor coolant system (RCS) average temperature was 582°F, RCS pressure was 2150 psig and pressurizer level was 220 inches, all within the normal range. The integrated control system (ICS) was also functioning normally when, at 4:14 a.m., a number of alarms sounded in the control room. One of the alarms was the "ICS or Fan Power Failure" alarm which indicated that there was a problem with the ICS.

### 4.2 Loss of the Integrated Control System DC Power

The loss of the ICS dc power was caused by a failure in the ICS power supply monitor which opened the two switches (S1 and S2) which supply 120 Vac power to the ICS.

When power was lost to the ICS, the plant responded as it was designed: the turbine bypass valves (TBVs), atmospheric dump valves (ADVs), main and startup



main feedwater (MFW) flow control valves, and the auxiliary feedwater (AFW) (ICS) flow control valves went to the 50 percent open position. The MFW stop valves shut, while the MFW pump turbines slowed to minimum speed.

The operators quickly recognized that a transient had begun because of the rapid increase in reactor coolant system (RCS) pressure, and an "ICS Runback or Limit" alarm that normally indicates that the ICS is automatically decreasing plant power levels.

The Shift Supervisor quickly opened the pressurizer spray valve in an attempt to stop the RCS pressure increase. In addition, the ADVs (one operable for each steam generator) and TBVs had traveled to the 50 percent open position as a result of the loss of ICS power and were providing RCS cooling. Further, the loss of ICS power caused the MFW pumps to slow to minimum speed, closed the main feedwater stop valves and caused the startup MFW flow control valves to close by 50 percent. As a result, MFW flow was essentially lost when the MFW pumps reached minimum speed, a condition which the operators did not recognize. The ICS would normally begin inserting control rods automatically to reduce reactor power under the above RCS conditions; however, the loss of the ICS dc power prevented it from performing this function. Because of the rapid overheating of the RCS caused by the loss of MFW flow, neither opening the pressurizer spray valve, nor the effect of the open TBVs and ADVs were sufficient to reverse the increase in RCS pressure, i.e., the net result of all these actions was undercooling of the RCS.

#### 4.3 Plant Trip and RCS Cooldown

The transient proceeded per design following a loss of ICS dc power. The operators responded promptly to plant conditions; however, they overlooked an alternate means of isolating the TBVs and ADVs which resulted in additional plant cooldown. The operators were also misled by an erroneously high MFW flow indication which, although it misled the operators, did not have a significant effect on the incident.

Due to the net undercooling, the reactor tripped (automatically shutdown) on RCS high pressure 16 seconds after the loss of ICS power. The RCS pressure peaked about 1 second later at 2298 psig, or 148 psig above normal operating pressure (152 psig below the pilot operated relief valve (PORV) setpoint). Several of the steam generator code safety valves lifted and then reseated. The reactor trip also generated a signal to trip the main turbine-generator. The operators closed the pressurizer spray valve upon reactor trip in anticipation of RCS cooldown and resultant depressurization.

Both AFW pumps actuated about the time the reactor tripped due to the low MFW pump discharge pressure. These pumps began to supply AFW flow to both steam generators through the 50 percent open AFW (ICS) flow control valves.

The operators recognized approximately 2 minutes after reactor trip that the plant had lost ICS power, but they did not recognize why it was lost nor did they initially understand the plant response to this loss of power. In this period, the failure of most ICS control stations to the 50 percent position, and the loss of all lights at these stations, were noted and led the control room operators to conclude that there had been a loss of ICS power. (See Section 5.1 for a discussion of the troubleshooting of the ICS.)

The operators also soon recognized the beginning of an overcooling transient due to the 50 percent demand to the TBVs, ADVs, and AFW (ICS) flow control valves. However, they realized that because of the loss of power to the ICS, they could not operate these valves from the control room. Therefore, nonlicensed operators were sent to various locations throughout the plant to close or isolate these valves manually. (Operators could have shut the ADVs and TBVs more quickly from the remote shutdown panel, and the ADVs could have been shut from the ADV manual control station. However, the operators overlooked these methods and instead proceeded to close or isolate all valves locally using valve handwheels.)

Operators in the control room also noticed pressurizer level decreasing, another indication of an overcooling transient, and fully opened the A high pressure injection (HPI) valve for more makeup flow to the RCS. The makeup tank (MUT) level began decreasing rapidly because of the increased makeup flow. Operators then opened the borated water storage tank (BWST) suction valve to the makeup pump to provide an additional source of makeup water and started the B HPI pump to increase makeup flow to the RCS from the BWST.

Believing that significant MFW flow existed, the operators in the control room then tripped both MFW pumps. The AFW pumps had already started and AFW flow was greater than 1000 gpm to each steam generator. The operators had noted that the MFW flow indication on the control room strip charts was at mid-range. It was indicating a flow of about 3 million pounds per hour. However, this MFW flow indication, which depended on ICS power, was in error. The actual MFW flow rate had decreased to zero because of the pressure in both steam generators and the low speed (approximately 2500 rpm) of both MFW pumps.

The Shift Supervisor in the control room could hear the roar caused by release of steam from the ADVs on the main steam lines; however, he could not determine the sources of all the steam releases. He recalled that the No. 4 MFW heater relief valve had been the source of a significant steam release and an overcooling transient twice previously: on October 2, 1985 and on December 5, 1985. Those releases were caused by a problem with both the auxiliary steam control valve supplying the No. 4 MFW heater and the No. 4 MFW heater relief valve. The Shift Supervisor therefore directed that the auxiliary steam control valve be isolated. The valve was shut from the control room. However, this still left the operators attempting to manually shut eight valves (four TBVs, two ADVs, two AFW (ICS) flow control valves) in four different locations in the plant (the two AFW (ICS) flow control valves, although physically only about 30 feet apart, are located in two separate areas because they are separated by a controlled area fence).

#### 4.4 SFAS Actuation, Continued Plant Cooldown and Partial RCS Depressurization

The safety features actuation system (SFAS) actuated on low RCS pressure in accordance with the plant design. RCS cooldown and depressurization, however, were rapid.

In a little less than 3 minutes after the reactor trip, RCS pressure decreased from 2298 psig to the SFAS setpoint of 1600 psig and pressurizer level had

decreased from 220 inches to 15 inches. The SFAS then automatically initiated and opened four HPI injection valves to predetermined positions. Selected SFAS equipment, including the motor-driven AFW pump, were automatically shed from the vital buses and sequence loading of SFAS equipment began. The AFW (SFAS) flow control valves fully opened. The BWST suction valves to the HPI pumps opened. The makeup tank suction valve and the HPI pump recirculation valve to the makeup tank (MUT) both isolated. The A and B low pressure injection/decay heat removal (LPI/DHR) pumps started in the recirculation mode. The diesel generators started but (as designed) did not load onto the vital buses because there was not a loss of power to the vital buses. The A HPI pump also started on the SFAS signal. The B HPI pump received a start signal; however, it was already operating. Both HPI pumps and the makeup pump were now operating in the HPI mode; nevertheless, RCS pressure continued to decrease.

The operators recognized that AFW flow was excessive and overrode the SFAS signal to the AFW (SFAS) flow control valves and closed them. However, the AFW (ICS) flow control valves remained at the 50 percent open position. Meanwhile, the motor-driven AFW pump automatically sequenced back on its vital bus and restarted. The dual-drive AFW pump had been running continuously and was powered by steam since it initially started.

The Shift Technical Advisor (STA) arrived in the control room approximately 6 minutes after the reactor trip after having gone to the turbine deck to determine which relief valves had lifted. He first checked the plant status and discussed the plant status with the Shift Supervisor.

The Shift Supervisor dispatched one of the Senior Reactor Operators (The "backup" Shift Supervisor) to help the Equipment Operators in the plant isolate the steam release and then turned his attention to restoring ICS power. A computer technician had been sent earlier to check the ICS power supply. The technician reported that all four ICS 24 Vdc power supplies were de-energized. He also reported that the automatic bus transfer (ABT) feeding the 120 Vac ICS power had not transferred and was still on the 1C bus (a vital bus), which was still energized. During the next 20 minutes, the Shift Supervisor, the Senior Control Room Operator and the Shift Technical Advisor also inspect the ICS power supplies, but they did not recognize that the switches (S1 and S2) feeding the 24 Vdc ICS power supplies, which are clearly marked, were both off. (See Section 6.7 for a more detailed discussion of this aspect of the incident.)

Meanwhile, the cooldown continued and steam generator pressures decreased to 500 psig. At this pressure the running condensate pumps began to supply feedwater to the steam generators through the idle MFW pumps and the 50 percent open startup MFW flow control valves. This feedwater initiation added approximately 1000 gpm of flow to each steam generator which continued to receive AFW flow. The RCS temperature had cooled 100°F in the first 7 minutes following the reactor trip. Later, the RCS pressure dropped to a low of 1064 psig (RCS temperature was 464°F), and the pressurizer water level decreased to off-scale low. (A subsequent evaluation indicated that a small steam bubble formed in the upper head region of the reactor vessel.)

The A and B control room/technical support center (TSC) heating, ventilation and air conditioning (HVAC) units started on the SFAS signal. Their operation

significantly increased the noise level in the control room, which interfered with the communications between the operators. Both HVAC units were later stopped. The SFAS also actuated containment (i.e. reactor) building isolation. This actuation isolated suction to the containment building radiation monitors, which later caused one of the associated sample pumps to overheat and smoke. This smoke in turn caused fire alarms to sound and caused isolation of the auxiliary building ventilation later during the incident.

#### 4.5 Excessive Plant Cooldown and Partial RCS Repressurization

The RCS continued to cooldown rapidly for the next 19 minutes; in all the temperature dropped 180°F in 26 minutes. During this period, the RCS repressurized to 1616 psig before starting to depressurize again. The items of greatest interest during this excessive cooldown period include: (1) the problems operators encountered while attempting to isolate AFW flow, (2) the discovery of the cause for ICS dc power loss, (3) the decision not to trip the AFW pumps and subsequent steam generator overfill, (4) the extent of HPI throttling and its effects on reactor coolant system repressurization and subcooling margin, and (5) a personnel error that resulted in closing the last open suction valve to the operating makeup pump.

The transient continued with the pressurizer level off-scale low, and with full HPI injection in progress. The operators outside the control room were working feverishly to isolate the sources of released steam and the excessive AFW flow. Although pressurizer level was off-scale low, the RCS subcooling margin was substantial (85°F and increasing). The subcooling margin (as measured in the RCS hot leg) began to increase prior to the reactor trip and did not decrease to the pre-trip value of 40°F at any time during the transient. The high subcooling margin while the pressurizer level was off-scale low was an indication to the operators that the pressurizer had not completely emptied. (However, as noted earlier, subsequent evaluations after the incident indicate that the pressurizer did completely empty and a small bubble formed in the reactor vessel head. The pressurizer was empty for approximately 3 minutes.)

Although the cooldown continued, the combined flow capacity of the two HPI pumps and the makeup pump apparently began to refill the pressurizer, although the level was still below the indicating range. RCS pressure also began to increase from a low point of 1064 psig. The continued cooldown, combined with the RCS pressure increase, resulted in RCS conditions that exceeded the B&W-designated temperature/pressure limits for pressurized thermal shock (PTS) of the reactor vessel (i.e. the PTS region) (See Figure 4.6). However, the nil ductility temperature (NDT) limits in the Rancho Seco Technical Specifications were not violated during this event. (See Section 8 for a more detailed discussion of this aspect of the incident.)

The control room operators throttled the A HPI flow slightly; however, RCS pressure and RCS subcooling margin continued to increase. The RCS subcooling margin at this time was well above the minimum requirement. This was the only instance of HPI throttling until pressurizer level came back on scale. The cooldown had now decreased steam generator pressures to about 435 psig, causing the main steam line failure logic to actuate. This actuation closed the startup MFW flow control valves, stopping MFW flow from the condensate pumps. This flow had lasted for approximately 2 minutes.

Nine minutes after being dispatched by the control room, the operators at the TBVs and the ADVs reported that the valves had been isolated. However, the nonlicensed operator at the AFW (ICS) flow control valves was experiencing some difficulty in closing them. He used the valve handwheel to partially close the B AFW (ICS) flow control valve, although he thought he had completely closed the valve. As a result, the flow to the B steam generator decreased by about 40 percent. He then went to the A AFW (ICS) flow control valve and closed it completely with the valve handwheel. Closing this valve completely caused the flow through the B AFW flow control valve to increase because much of the flow through the A AFW (ICS) flow control valve was apparently redirected through a line crossconnecting the two valves. However, the operator believed that the A AFW flow control valve was only 80 percent closed since he could still see about 1/2-inch of uncorroded valve stem. Using a valve wrench, he applied additional force to the valve, which resulted in failure of the manual operator, whereupon the valve reopened. As a result, local manual control of the valve by the valve handwheel was no longer possible.

In the meantime, a second nonlicensed operator arrived at the B AFW (ICS) flow control valve and subsequently closed it completely. The first operator then called the control room and was told to close the A AFW manual isolation valve. Since it would not move, even after he applied a valve wrench, it remained open. The A AFW (ICS) flow control valve also remained open until ICS power was restored. Because of its location, the second operator found it expeditious to jump a controlled area fence approximately 6 feet high when going from the B to the A AFW (ICS) flow control valves. This appeared to have saved about 2 minutes. (See Sections 5.2 and 5.3 for a more detailed discussion of the valve failures.)

Although position indicators are mounted alongside the AFW flow control valve stem, operators did not use them to determine the valve position. Even if they had been used, however, the accuracy of these indicators is questionable due to the poor gradation and marking on the scale and because of a 1/8-inch separation on indicator discs. In addition, the position indicator is located such that the operator cannot see it directly while operating the handwheel.

The operators at the AFW (ICS) flow control valves also experienced difficulty in communicating with the control room. The operators tried to use portable two-way radios, but they did not function in this area. Finally, the operators used a telephone more than 100 feet from the valves to call the control room.

Meanwhile, in the control room, pressurizer level was back on scale and increasing so that operators started to throttle all the HPI valves to slow the increase in RCS pressure. The subcooling margin was 170°F.

The operators opened the HPI pump SFAS-controlled recirculation valves to prevent the pumps from overheating when flow was subsequently further throttled. However, the suction valve from the makeup tank was still closed at this time. Recirculation flow was sent to the makeup tank, which soon filled, and the relief valve began to discharge to the flash tank.

The operators in the control room stopped the C reactor coolant pump (RCP) and the A HPI pump at an RCS temperature of 418°F. (Procedures require that no

more than three RCPs operate below 500°F, due to core-lift considerations.) Thus, operation of the fourth RCP below 500°F appears to have been a contrary to plant procedures. The RCS pressure was still increasing and soon peaked at 1616 psig. The C and D HPI injection valves were then closed to reduce the repressurization and the pressurizer spray valve was opened in an attempt to depressurize to outside the PTS region.

The Shift Supervisor declared an Unusual Event at 4:30 a.m. and directed the Senior Control Room Operator to notify State, and county authorities. He also requested the STA to telephone various Rancho Seco shift and management personnel get them to the plant.

The Shift Supervisor, STA and the Senior Control Room Operator had earlier discussed whether the AFW pumps should be tripped. The emergency procedures had been modified after the cooldown transient of October 2, 1985 to require that the AFW pumps be tripped during an overcooling transient if the steam generator could not be isolated by shutting valves. The Shift Supervisor, however, made the decision to delay tripping the AFW pumps. The operators were concerned that AFW might not be available, when later required, if the AFW pumps were tripped.

Meanwhile, the strip charts indicated that the A steam generator was overflowing with the overflow entering the steam lines. The safety parameter display system (SPDS) video screen also showed steam generator levels and this indication was later reported to have indicated the steam generators were not full. (Subsequent testing, however, indicates that the strip charts and the SPDS video indications were in close agreement.) The A steam generator actually filled to the top of the steam shroud and began to spill water into the steam annulus and into the mainsteam line for about 7 minutes until ICS power was restored. The AFW flow rate to the A steam generator at this time was off scale high (i.e., greater than 1300 gpm). (A later evaluation and inspection showed there was no apparent damage to the main steam lines or the turbine driven AFW pump as a result of this overflow.) (See Section 6.5 for a more detailed discussion of the operators' concern about stopping the AFW pumps.)

The MUT was still receiving the HPI pump recirculation flow and, in turn, was relieving to the flash tank. The control room operators, therefore, closed the suction valve from the BWST in an attempt to mitigate the high level in the MUT, forgetting the suction line from the MUT was shut. This action isolated the suction to the makeup pump, the A HPI pump (which had been stopped earlier), and the A LPI/DHR pump, which was in recirculation.

While the steam releases had been isolated earlier, the A AFW (ICS) flow control valve was still open which produced an RCS cooldown rate of approximately 200°F per hour. The RCS subcooling margin peaked at 201°F at 4:39 a.m. at an RCS temperature of 390°F and an RCS pressure of 1430 psig. This was about 800 psi higher than the pressure limit for the PTS region at this temperature (see Section 6.4 for a more detailed discussion of the dichotomy between regaining pressurizer level and avoiding the PTS region).

Finally, at 4:40 a.m. the "backup" Shift Supervisor had arrived back in the control room after having helped to isolate the steam release and discovered that switches S1 and S2 to the ICS dc power supplies were tripped to the OFF position.

#### 4.6 Restoration of ICS DC Power and Plant Stabilization

Twenty-six minutes after it was lost, ICS dc power was restored when switches S1 and S2 were turned back to the ON position. With power restored, normal remote control of ICS equipment in the control room also was restored. Shortly after ICS power was restored, the Senior Control Room Operator (SCO) called the NRC Operations Center and reported an Unusual Event. The SCO briefly described the event and promised to call back later with additional details. The operators were now able to stop the RCS cooldown and continue to depressurize out of the PTS region. The main items of interest during this period were the damage to the makeup pump, which subsequently released radioactivity, the illness of the "backup" Shift Supervisor, and an additional loss of ICS dc power.

When power to the ICS was restored, apparently all the ICS-controlled valves shifted to the manual mode and received a demand signal to go fully open, a condition that was unexpected by the operators. However, the isolation valves for the TBVs and ADVs had been closed and the B AFW (ICS) flow control valve had been shut with the handwheel. The control room operators immediately shut all open ICS-controlled valves, including the open A AFW (ICS) flow control valve, remotely from the control room. All AFW flow to both steam generators was now stopped, and the RCS began to heat up. The lowest RCS temperature reached was 386°F. (The plant had cooled by 180°F in 26 minutes.)

At this time, RCS pressure was being reduced to achieve conditions outside the PTS region. The operators were directed to disengage the manual handwheel on the B AFW (ICS) flow control valve and to open the isolation valves for the ADVs and TBVs so that the ICS could completely resume control of these valves. The A steam generator level decreased below the steam shroud level shortly after the A AFW (ICS) flow control valve was shut.

The RCS cooldown had largely stopped so operators stopped the B HPI pump and closed the open HPI injection valves (A and B). However, they left the makeup pump operating. The A HPI pump had been stopped earlier. The operators at this time attempted to restore normal makeup flow through the makeup valve; however, the makeup isolation valve could not be opened from the control room because the operators did not reset one of the SFAS isolation signals for this valve.

Shortly after stopping the B HPI pump, the operators noticed a loss of RCP seal flow (they received an alarm and low flow indication) and restarted the B HPI pump to re-establish seal flow. The operators checked the valve lineup to the seals and again stopped the B HPI pump. However, flow to the seals again stopped and the B HPI pump was restarted. What the operators did not realize was that the makeup pump was severely damaged and could not supply adequate RCS seal injection flow. (The A LPI/DHR pump was apparently not damaged since it was operating with its recirculation line open and therefore discharging back to its own suction.)

Coincident with this seal flow problem, the auxiliary building stack radiation monitor alarmed. A smoke alarm was also received that isolated the auxiliary building ventilation system. The inadequate seal flow and radiation alarms were apparently all caused by the failure of the makeup pump that had been operating for about 10 minutes with both suction valves (i.e., BWST and MUT) closed. At 5:00 a.m., the operators in the control room heard a loud noise, observed that the makeup pump ammeter was reading only about 1/3 of normal running

current, and then realized that the makeup pump had been damaged. They also then realized that both makeup pump suction valves were closed and immediately opened the suction valve from the MUT in the hope of preventing further damage to the pump. Opening the valve allowed water to spill from the damaged makeup pump onto the pump room floor. Operators closed the valve after approximately 450 gallons had spilled. (See Section 6.7 for a more detailed discussion of the makeup pump failure.)

The failed makeup pump had only a single stop-check valve that isolated the RCS from the failed makeup pump seals. In addition, the makeup pump was isolated from the operating HPI pump recirculation line by only a single stop-check valve. Consequently, there was some concern on the part of the Control Room Operators that this failure could lead to a small break LOCA. Therefore, the Shift Supervisor sent two nonlicensed operators to enter the makeup pump room and isolate the makeup pump by closing the locked open manual isolation suction and discharge valves and the manual recirculation line isolation valve. The makeup pump room contained airborne radioactivity and about 4 inches of radioactively contaminated water on the floor. Although the operators wore some protective clothing, they did not wear respirators or high top boots because none were available near the pump room entrance. The operators performed a radiation survey before entering into the makeup pump room, however, no assessment was made of particulate or gaseous radioactivity until after they entered.

After isolating the makeup pump, the operators entered the west decay heat cooler room to attempt to open the SFAS-actuated makeup isolation valve by hand. This valve still had a "close" signal so that they were unable to open it. Operators later found that the SFAS signal had not been reset for the makeup isolation valve at the B safety features panel. (Following actuation of the SFAS, the makeup valve "close" signal must be cleared at both the A and B safety features panels.) The operators then went back into the makeup pump room briefly to check the status and then left the area. (Both operators were monitored and whole body counted on the morning of December 26. The results showed that they had not received a significant radiation dose from the entry into the makeup pump room.)

Meanwhile, the "backup" Shift Supervisor became ill in the control room and collapsed in front of the control panel. He had assisted in isolating the ADVs, which are located outside where the weather was cold and damp. At this time an additional SCO arrived at the plant. He was not scheduled to be on shift and had arrived early to do some paperwork. When he reached the control room, he turned his attention to the operator who had become ill. After discussing the situation with the Shift Supervisor, he called an ambulance. The operator was later transported to the hospital and then released. The operator's illness required the attention of the control room operators and resulted in the loss of one plant operator, although it did not have a significant effect on the incident. (SMUD stated during the Team's investigation that, based upon the medical diagnosis at the hospital and other information, there was no indication that drugs or alcohol were involved.)

After calling the ambulance, the off duty SCO answered the Emergency Notification System (ENS) phone when the NRC Operations Center called and requested an update on the plant's initial report. After the SCO briefed the NRC Operations Center, he was requested to maintain an open line. The open line was maintained until the Unusual Event was later terminated. Operators in the control room



were intent on stabilizing the plant and bringing all systems and parameters to normal where possible. The RCS had now depressurized out of the PTS region and a 3-hour soak at the existing RCS temperature and pressure (870 psig and 428°F) was begun in accordance with B&W guidelines. Operators began to drain the overfilled steam generator to the condenser to re-establish MFW flow with the main condensate pumps.

The Shift Supervisor became concerned about the habitability of the auxiliary building after the ventilation system shutdown, so he decided to restart the ventilation system. However, a smoke detector alarm in the radiological waste area prevented the ventilation system from operating. The smoke detector in the radiological waste area is believed to have detected smoke from the reactor building radiation monitor, which overheated when its suction was isolated by the SFAS actuation. Efforts to start the auxiliary building ventilation system were finally successful and ventilation from the auxiliary building to the atmosphere was restored. (The maximum permissible radionuclide concentration at the site boundary was later calculated to be less than one-fifth of the maximum permissible concentration for 1 hour. The whole body dose to a person hypothetically at the site boundary during the event would have been no greater than 0.2 mrem. The thyroid dose would have been 0 mrem. These results are well within Rancho Seco Technical Specification limits.)

After assisting in isolating the makeup pump, a nonlicensed operator noticed he had lost his security badge. Thus, he was no longer able to open doors to the areas that require a badge for entrance. After reporting the loss to the control room, he was escorted by a security guard to the control room where he remained until a spare security badge was brought to him about 20 minutes later.

The SFAS signal was also "bypassed" at 6:06 a.m. At approximately 6:10 a.m., the plant was stabilized. The main steam line failure logic had been "inhibited" and the steam generators were being fed by the main condensate pumps.

At 6:11 a.m. a momentary "ICS or Fan Power Failure" alarm occurred. The S1 and S2 switches remained closed and the alarm cleared without operator action. No equipment response was noted.

At 6:14 a.m., a third "ICS or Fan Power Failure" alarm was received. The ICS-controlled valves received 50 percent demand signals. Operators immediately reset switches S1 and S2 to restore ICS power, after which the ICS-controlled valves received 100 percent demand signals. The operators then shut the valves remotely from the control room.

The Plant Superintendent relieved the Shift Supervisor as Emergency Coordinator and manned the Technical Support Center (TSC) at 7:15 a.m. Meanwhile, several gallons of water had spilled onto the TSC floor. The water came from a drain on a pilot-operated valve in the fire main when a fire alarm was received and the normally dry fire header was pressurized with water. There was no release of water from the fire main itself and the spilled water had no significant effect on this incident.

The SMUD Emergency Coordinator terminated the Unusual Event at 8:41 a.m.

Table 4.1 Chronological Sequence of Events

---

Plant Status and Oncoming Shift

---

- Unit was operating at steady state power of 76% [712 MW(e)].
- Reactor Coolant System (RCS) average temperature was 582°F.
- RCS pressure was 2150 psig.
- This plant does not have main steam isolation valves (MSIVs).
- The plant had returned to power on December 24, 1985 following an outage of 2 days.
- Integrated Control System (ICS) was in full automatic.
- The Bailey computer was out of service (one of the plant's two main computer systems in the control room). Consequently, the Bailey post-trip review, Bailey alarms printout, and Bailey inputs to the interim data acquisition and display system (IDADS) were not available. IDADS inputs from sources other than the Bailey computer were available.

Transient Initiator - Loss of ICS DC Power

- 04:13:47 Loss of ICS dc power which caused an "ICS or Fan Power Failure" annunciator alarm and an "ICS Runback or Limit" alarm. The loss of ICS power was caused by failure of the ICS power supply monitor which opened the two switches (S1 and S2) which supply power to the ICS dc power supply modules.
- 04:13:+ Control room operators noticed MFW flow decreasing rapidly. This was caused by the runback of the MFW pumps to minimum speed and partial closing of the main MFW flow control valve. Also, they noticed RCS pressure increasing. The Shift Supervisor opened the pressurizer spray valve in an attempt to stop the RCS pressure increase.
- 04:14:01 The automatic runback of MFW pump speed caused (per design) a low MFW pump discharge pressure of less than 850 psig which automatically started the motor driven AFW pump.

Plant Trip and Start of Cooldown

- 04:14:03 The reactor tripped on high RCS pressure. The turbine trip was also initiated by the reactor trip. The pressurizer spray valve was closed remotely from the control room in anticipation of RCS cooldown and depressurization.
- 04:14:04 The plant reached a peak RCS pressure of 2298 psig. Six OTSG code safety valves lifted and later reseated.

Table 4.1 Chronological Sequence of Events (Cont.)

---

04:14:06	AFW dual drive (i.e. steam and electric) pump automatically started on low MFW pump discharge pressure.
04:14:06	The plant reached a peak RCS hot leg temperature of 606.5 F.
04:14:+	The operators performed the steps of the Emergency Operating Procedure E.01 (Reactor Trip Immediate Actions). This included reducing RCS letdown flow. Operators then proceeded with Emergency Operating Procedures E.02 (Vital System Status Verification).
04:14:11	AFW flow began to both OTSGs through the 50% open AFW (ICS) flow control valves.
04:14:25	Operators noted pressurizer level decreasing, and fully opened the A HPI injection valve for more makeup flow to RCS.
04:14:30	The loss of ICS dc power also resulted in loss of remote control of ICS-controlled valves from the control room.
	The operators soon recognized the beginning of an overcooling transient due to the 50% demand to the TBVs, ADVs, and AFW (ICS) flow control valves. However they also realized that because of the loss of power to the ICS, they could not remotely operate these valves from the control room. Therefore, nonlicensed operators were sent to various locations to close or isolate these valves. The operators went directly to the affected valves and attempted to close or isolate all valves locally by using handwheels.
04:14:48	Makeup tank (MUT) level started decreasing rapidly. Operators opened the suction valve from the borated water storage tank (BWST) to the makeup pump to provide an additional source of makeup water.
04:15:04	Operators started the B HPI pump to increase makeup flow to the RCS from the BWST.
04:16:02	The operators in the control room tripped both MFW pumps. The AFW pumps had already started and AFW flow was greater than 1000 gpm to each OTSG. The operators had noted the MFW flow indication on the control room strip charts which indicated flow of about 3 million pounds per hour. The actual MFW flow rate decreased to zero due to the pressure in both OTSGs and the low speed (approximately 2500 rpm) of both MFW pumps. In addition, the MFW stop valves were shut although there was still a flow path through the partially open startup MFW flow control valves.

Table 4.1 Chronological Sequence of Events (Cont.)

---

SFAS Actuation, Continued Plant Cooldown and Partial RCS Depressurization

- 04:16:57 RCS pressure had decreased from 2298 psig to the SFAS setpoint of 1600 psig and pressurizer level had decreased from 220 inches to 15 inches. SFAS automatically initiated and the four HPI injection valves opened to predetermined positions. Selected SFAS equipment, including the motor-drive AFW pump, were automatically shed from the vital buses and sequence loading of SFAS equipment began. The AFW (SFAS) flow control valves travelled full open. The BWST suction valves to the HPI pumps opened. The makeup tank suction valve and the HPI and makeup pump combined recirculation valves closed. The A and B low pressure injection/decay heat removal (LPI/DHR) pumps started in the recirculation mode. The diesel generators started but, as designed, did not close onto the vital buses as there was not a loss of power to the vital buses.
- 04:16:59 The A HPI pump started on the SFAS signal. The B HPI pump received a start signal; however, it was already operating. Both HPI pumps and the makeup pump were now operating in the HPI mode; however, RCS pressure continued to decrease.
- 04:17:10 Operator overrode the SFAS signal to the AFW (SFAS) flow control valves and closed them.
- 04:17:15 A and B control room/technical support center (CR/TSC) essential heating, ventilation and air conditioning (HVAC) units started on the SFAS signal. This significantly increased the noise level in the control room.
- 04:17:27 The motor-driven AFW pump automatically sequenced back on its vital bus and restarted. The dual-drive AFW pump had been running continuously and powered by steam since it initially started.
- 04:18:58 RCS temperature decreased below 500°F.
- 04:19 The pressurizer emptied and steam began to form in the upper reactor vessel head.
- 04:19:15 Operators secured A CR/TSC essential HVAC to reduce the noise level in the control room.
- 04:20 The STA arrived in the control room after having gone to the turbine deck to determine which relief valves had lifted.
- 04:20:00 Pressurizer level was off-scale low. Subcooling margin was 85°F and increasing.

Table 4.1 Chronological Sequence of Events (Cont.)

- 
- 04:20:+ The Shift Supervisor sent a computer technician to check the ICS power supply. The technician reported that all four ICS 24 Vdc power supplies were de-energized. The automatic bus transfer (ABT) had not transferred and was still on the C bus (vital bus) which was still energized. During the next 20 minutes, the Shift Supervisor the Senior Control Room Operator and the STA would also inspect the ICS power supplies, but each did not recognize that the power supply switches (S1 and S2) feeding the 24Vdc ICS power supplies were both OFF.
- 04:20:20 OTSG pressures had decreased to 500 psig. At this pressure the running condensate pumps began to supply feedwater to the OTSGs through the idle MFW pumps and the open startup MFW flow control valves. This added approximately 1000 gpm of flow to each OTSG. (It appears that the control room operators were not aware of this flow.)
- 04:21:25 Minimum RCS pressure of 1064 psig was reached, RCS temperature was 464°F.

Excessive Plant Cooldown and Partial RCS Repressurization

- 04:21:+ Although the cooldown continued, the combined flow capacity of the 2 HPI pumps and the makeup pump, along with the reactor vessel bubble, apparently began to refill the pressurizer, although the level was still below the indicating range. RCS pressure also began to increase from a low point of 1064 psig.
- 04:22 The plant exceeded the B&W-recommended temperature/pressure limits for pressurized thermal shock (PTS) of the reactor vessel (i.e., the PTS region). The nil ductility temperature (NDT) limits in the Technical Specifications were not violated during this incident.
- 04:22 An operator initially throttled HPI injection flow slightly. RCS pressure was beginning to increase, but pressurizer level was still off-scale low.
- 04:22:50 OTSG pressures had decreased to 435 psig. Main steam line failure logic actuated, which closed the startup and main MFW valves. Flow from the condensate pumps was stopped. (It appears that the operators may not have been aware of this.)
- 04:23 ADV and TBV isolation valves were shut locally (i.e., by handwheels) by operators.
- 04:23:10 A nonlicensed operator attempted to close B AFW(ICS) flow control valve using the valve handwheel. The valve was only partially closed by the operator. The operator thought he had completely closed the valve at this point. AFW flow to the B OTSG, however, had decreased by about 40%.

Table 4.1 Chronological Sequence of Events (Cont.)

- 
- 04:25:30 An operator opened the HPI pump SFAS-controlled recirculation valves, opening the recirculation path to the makeup tank to prevent overheating the pumps when flow was subsequently further throttled. However, the operators did not realize that the suction valve from the makeup tank was still closed at this time.
- 04:26:15 CR/TSC essential HVAC train B was secured to further reduce noise levels in the control room.
- 04:26:+ The nonlicensed operator attempted to close the A AFW (ICS) flow control valve using the valve handwheel.
- 04:26:22 The A AFW flow control valve closed. Operator believed it was only 80% closed and left to locate a valve wrench.
- 04:26:47 Pressurizer level was back on scale and increasing. Subcooling margin was 170°F. Operators throttled HPI injection valves to decrease the rapid increase of reactor pressure.
- 04:28:00 Makeup tank (MUT) level went offscale high. The MUT pressure relief valve opened and discharged to the flash tank.
- 04:28:00 The control room operators stopped the C RCP pump at an RCS temperature of 418°F. (The pump should have been stopped when pressure decreased below 500°F. Procedures require that no more than three RCPs operate below 500°F to preclude core lift.)
- 04:28:43 RCS letdown was restored.
- 04:28:59 Operators stopped the A HPI pump.
- 04:29:40 The nonlicensed operator used a valve wrench on the A AFW (ICS) flow control valve. The manual portion of valve operator was damaged. The valve suddenly failed open. The operator called control room and was told to close the A AFW manual isolation valve.
- 04:29:40 RCS pressure peaked at 1616 psig. RCS temperature was 418°F.
- 04:29:45 An operator reduced HPI flow by closing C and D HPI injection valves to reduce the repressurization while temperature was still decreasing.
- 04:30 The Shift Supervisor declared Unusual Event. The Senior Control Room Operator notified State and County agencies. The STA telephoned additional Rancho Seco personnel to get them to the plant.
- 04:30:30 Operators started depressurizing RCS using normal pressurizer spray in an attempt to return to condition outside PTS region.

Table 4.1 Chronological Sequence of Events (Cont.)

- 
- 04:33:20 A second nonlicensed operator arrived at the B AFW flow control valve and closed it all the way. AFW to the B OTSG was now stopped; however, much of this flow may have been diverted to the A OTSG.
- 04:33:40 The A OTSG was full to the top of the steam shroud and began to spill water into the steam annulus and into the main steam lines. At this time, the AFW flow to the A OTSG was in excess of 1300 GPM.
- 04:35 Operators closed the A HPI suction valve from the BWST in an attempt to draw more water from the MUT and reduce the high level in the makeup tank. However, the suction valve from the MUT was still shut.
- 04:36 The first nonlicensed operator attempted to close the A AFW manual isolation valve but it would not move, even with the valve wrench.
- 04:39:00 The RCS subcooling margin reached a peak of 201°F and began to decline. (RCS temperature = 390°F, RCS pressure = 1430 psig.) This was approximately 800 psi into the PTS region.

Restoration of ICS DC Power and Plant Stabilization

- 04:40 The "backup" Shift Supervisor discovered that the switches (S1 and S2) to the ICS dc power supplies were tripped OFF. ICS power was restored by closing switches S1 and S2 in the ICS cabinet. Remote (CR) control of ICS-controlled valves was restored. Initially the ICS-controlled valves shifted to the hand mode and received a demand signal to go fully open when power was restored. However, all but the A AFW flow control valve had been closed or isolated. The control room operators immediately shut all open ICS-controlled valves, including the damaged AFW(ICS) flow control valve.
- All AFW flow to both OTSGs had stopped. RCS began to heat up. The lowest RCS temperature of 386°F was reached and at this time RCS pressure (1413 psig) was being reduced to achieve conditions outside the PTS region. The plant had cooled down 180°F in 26 minutes.
- 04:41:00 The first nonlicensed operator called the control room and reported that the A AFW manual isolation valve was stuck open. The operators were directed to disengage the manual handwheel on the B AFW flow control valve. Other operators were directed to unisolate the ADVs and TBVs.
- 04:41:10 The A OTSG level decreased below the steam shroud.
- 04:42:42 An operator stopped the B HPI pump. The makeup pump continued to run.
- 04:42:56 Operators closed the A and B HPI injection valves.
- 04:43:50 An operator noted a loss of RCP seal injection flow.

Table 4.1 Chronological Sequence of Events (Cont.)

- 
- 04:43:54 An operator restarted the B HPI pump to re-establish RCP seal injection flow.
- 04:49: Leakage (steam) from the damaged makeup pump was released via the auxiliary building ventilation system. The auxiliary building stack radiation monitor alarmed and shifted exhaust to the charcoal filters. Smoke from the damaged makeup pump caused a fire alarm which isolated the auxiliary building ventilation system, stopping the release. The release was within Technical Specification limits.
- 04:50:19 An operator stopped the B HPI pump.
- 04:50:30 An operator again noticed loss of seal flow and restarted the B HPI pump. (Note: loss of RCP seal flow was due to the failure of the makeup pump. The operators were not yet aware of the failure.)
- 04:52 The "backup" Shift Supervisor collapsed in front of the control panel. This operator had previously assisted in closing the ADV and TBV manual isolation valves.
- 05:00 Operators in the control room heard a loud noise. They observed the makeup pump ammeter and noted it read about 1/3 of normal running current and realized the makeup pump had been damaged due to lack of suction.
- 05:00:10 An operator tripped the makeup pump. An operator opened the makeup tank suction valve, which allowed water to spill out of the damaged makeup pump onto the pump room floor. The operator subsequently shut the suction valve. Approximately 450 gallons were spilled.
- 05:05 RCS pressure decreased out of PTS region. A 3-hour soak was initiated. (RCS Pressure = 870 psig, RCS temperature = 428 F.)
- 05:05 An ambulance was called for the operator who collapsed.
- 05:09 Both AFW pumps were manually stopped while OTSG level was reduced via the OTSG drain lines to allow re-establishment of normal MFW flow with the condensate pumps.
- 05:27 Nonlicensed operators isolated the pump by entering the pump room which contained airborne radioactivity and 3 to 4 inches of contaminated water on the floor. The operators did not wear respirators or high-top shoe covers because they were not available in the area. They thus became contaminated from water on the floor.
- 05:29 The nonlicensed operators entered the west decay heat cooler room to attempt to manually open the SFAS-actuated makeup isolation valve. This valve still had a close signal, therefore they were unable to open it. It was later found that the SFAS signal had not been reset for the makeup isolation valve at the B safety features panel.



Table 4.1 Chronological Sequence of Events (Cont.)

---

05:29:04	Operators stopped the second (A) RCP.
05:33	A smoke detector locked-out rad waste area exhaust fans. This was apparently caused by smoke from the reactor building radiation monitor pump which was discovered overheating at 5:46 a.m.
05:40	Main steam line failure logic was inhibited. This permitted flow to the OTSGs from the condensate pumps.
05:46:	Operators discovered that the reactor building radiation monitor overheated due to shutting the suction valve when SFAS initiated and isolated the reactor building.
05:54	A nonlicensed operator lost his security badge. He was escorted to the control room by a security guard. The control room called security and requested that a spare security badge be brought to the control room.
06:06:00	Operators bypassed SFAS.
06:11	A momentary "ICS or Fan Power Failure" alarm was received. However, the S1 and S2 switches remained closed and the alarm cleared without operator action. No equipment response was noted.
06:14	On the "ICS or Fan Power Failure" alarm, ICS-controlled valves again received a 50% demand signals. Operators immediately reset switches S1 and S2 to restore ICS power. ICS-controlled valves again received a 100% demand signals. Operators remotely(CR) shut the valves from the control room.
06:15	Security personnel brought a spare security badge to the control room.
07:00	The SRO was released from the hospital.
07:15	The Plant Superintendent relieved the Shift Supervisor as Emergency Coordinator and manned the technical support center.
08:41	The Unusual Event was terminated by the SMUD Emergency Coordinator.

---

# REACTOR TRIP DEC. 26, 1985

RCS PRESSURE/PZR LEVEL

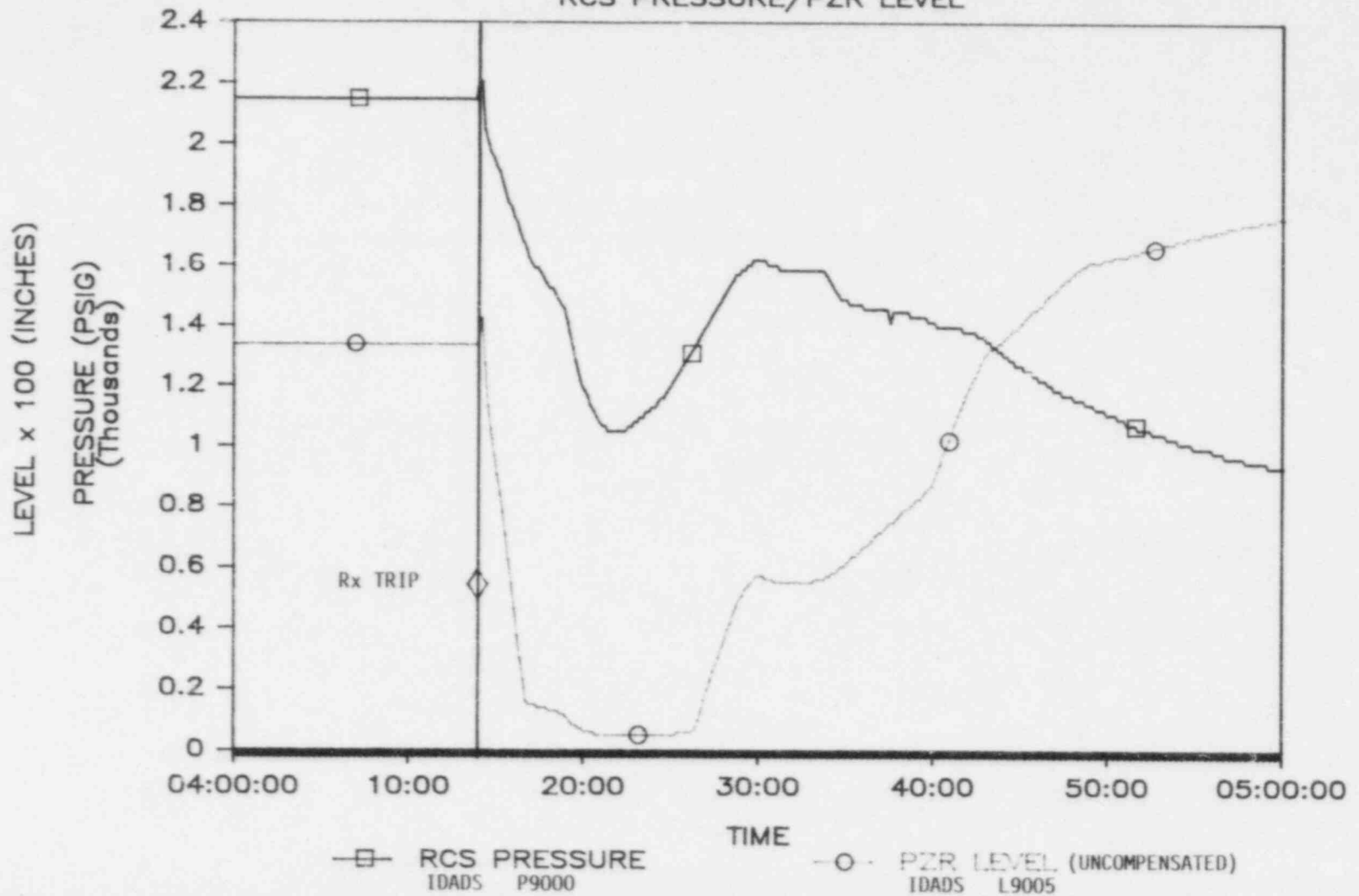


Figure 4.1 RCS pressure/pressurizer level from 4 a.m. to 5 a.m. on December 26, 1985

# REACTOR TRIP DEC. 26, 1985

RCS Tave / RCS PRESSURE / Tsat

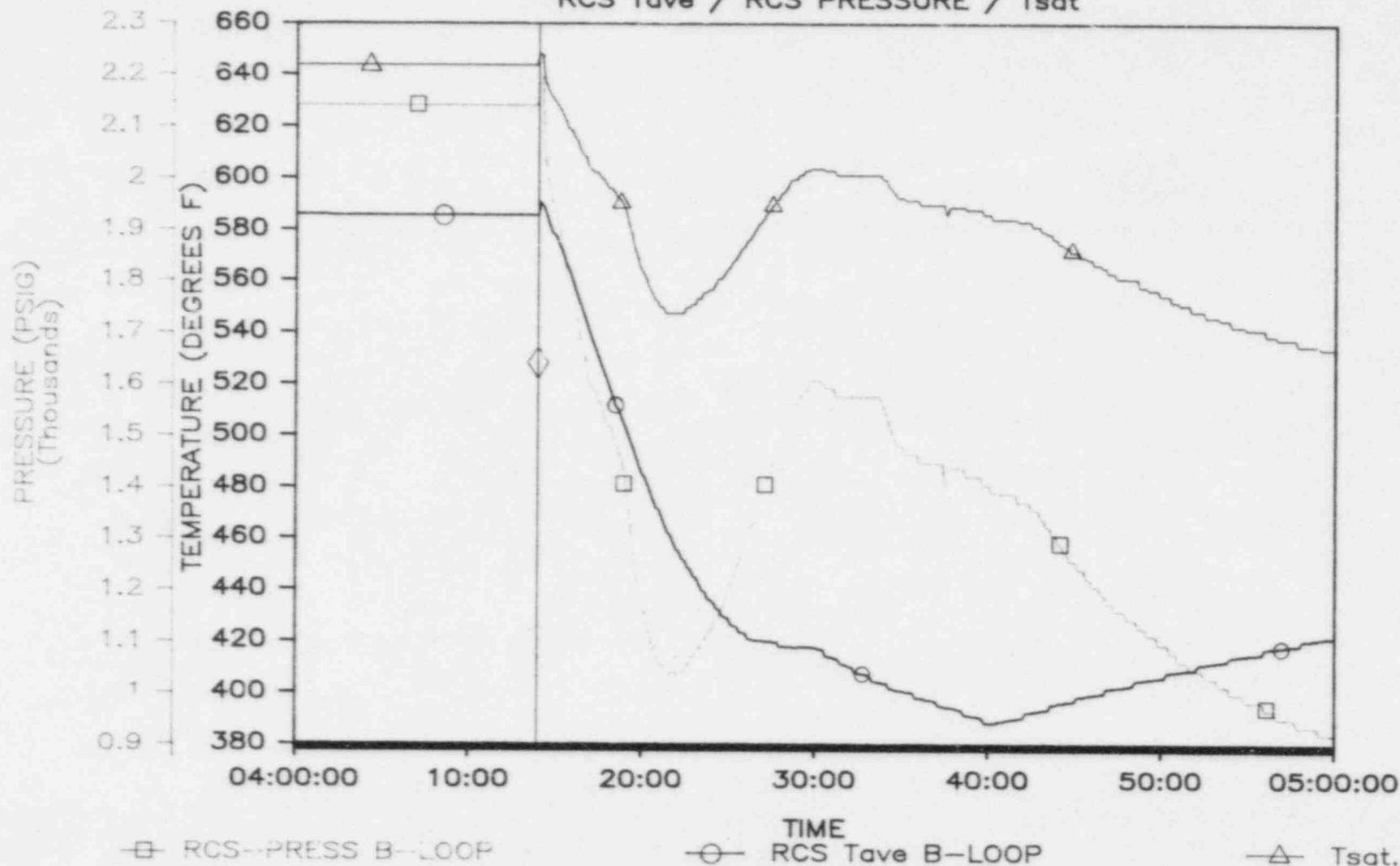


Figure 4.2 RCS pressure/temperature ( $T_{ave}$ )/RCS saturation temperature ( $T_{sat}$ ) on reactor trip from 4 a.m. to 5 a.m. on December 26, 1985

# REACTOR TRIP, DECEMBER 26, 1985

## AUX FEEDWATER FLOWRATES

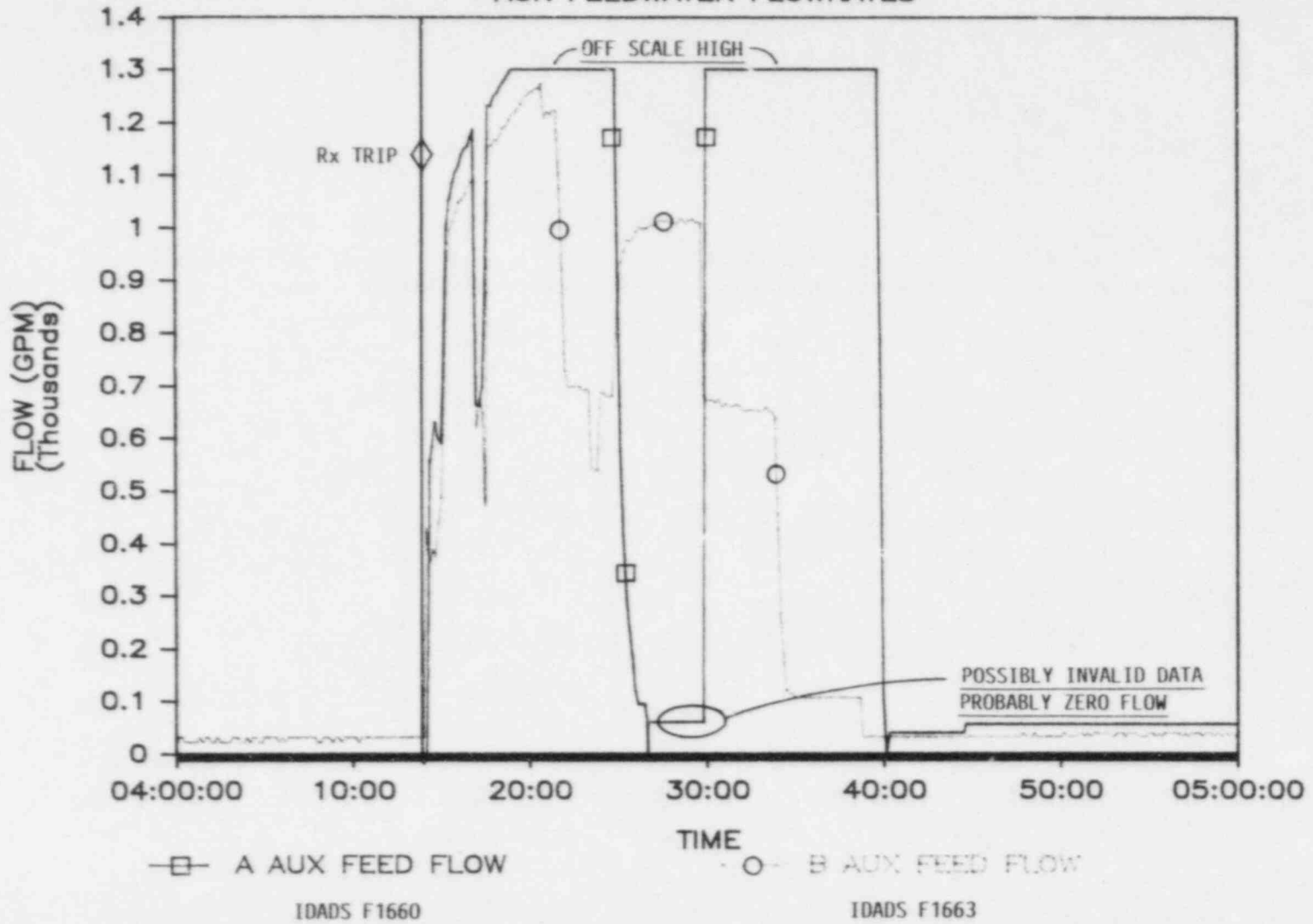


Figure 4.3 Auxiliary feedwater flow rates on reactor trip, December 26, 1985

# REACTOR TRIP DEC. 26, 1985

## HPI & MAKE UP FLOW

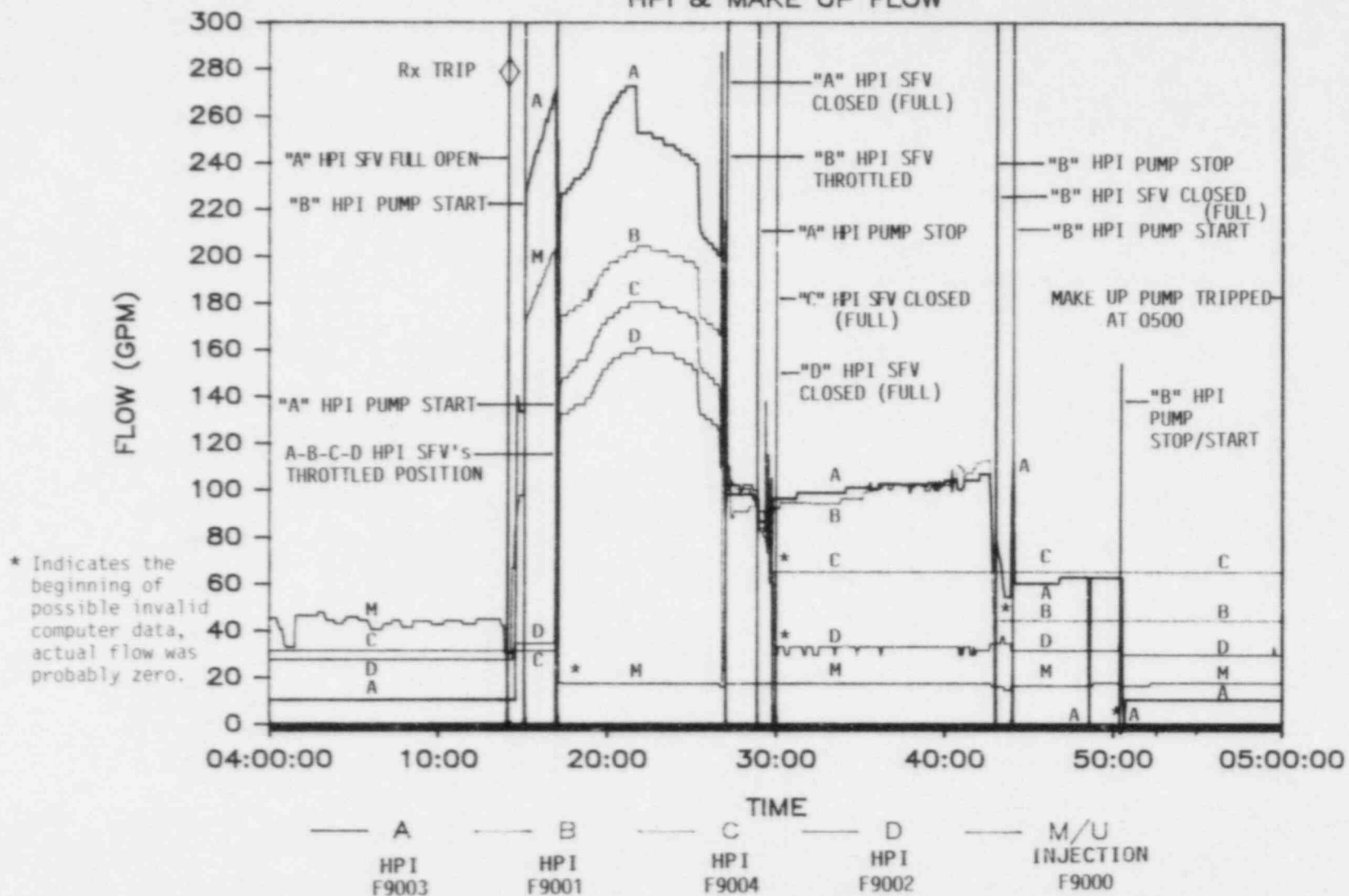


Figure 4.4 HPI and makeup injection flow rates on reactor trip, December 26, 1985

# REACTOR TRIP DEC. 26, 1985

## FULL RANGE OTSG LEVELS

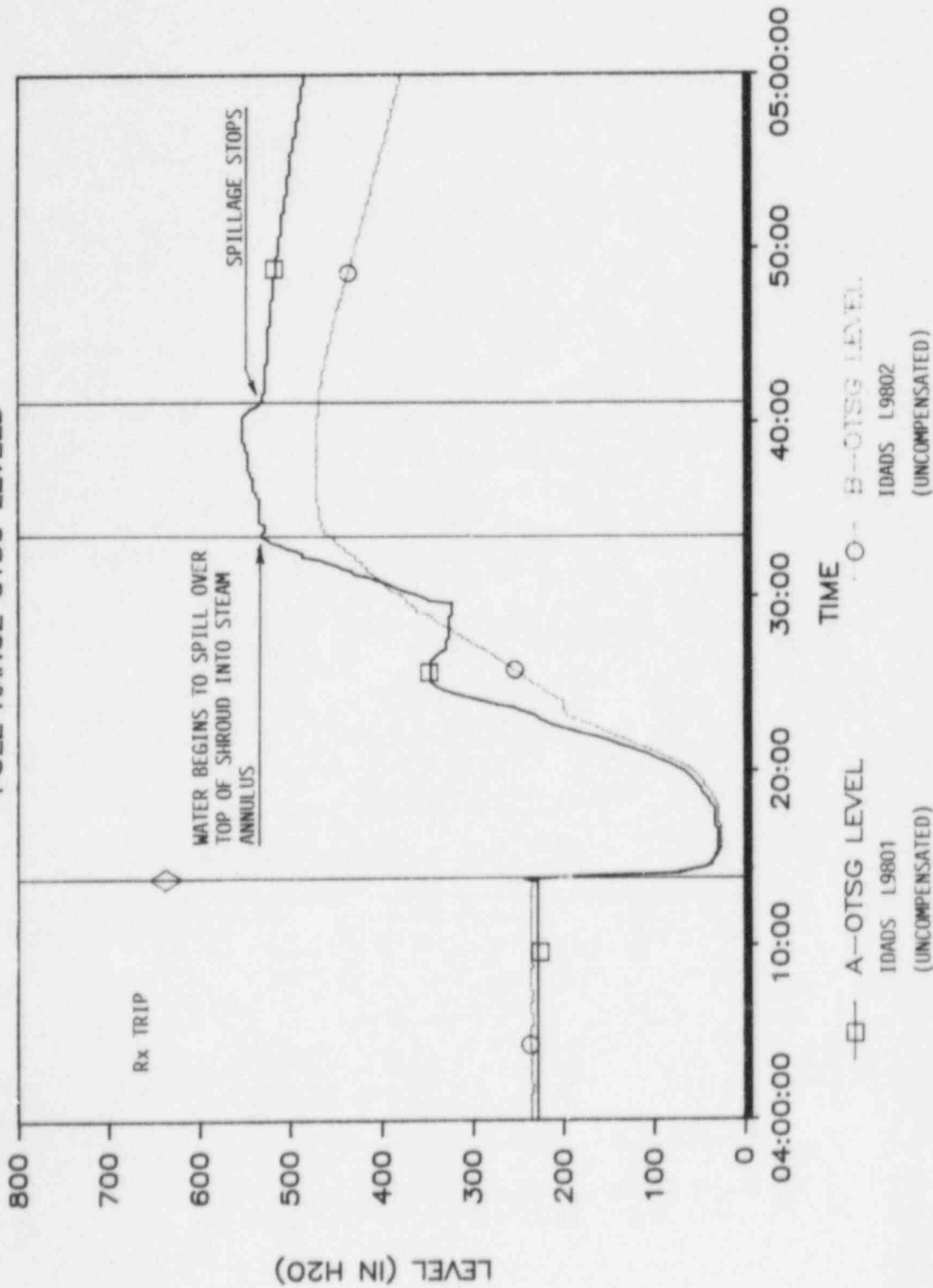


Figure 4.5 Full-range OTSG levels on reactor trip, December 26, 1985

# Rx TRIP COMPARISON

## PRESS-TEMP to TECH SPEC COOLDOWN CURVE

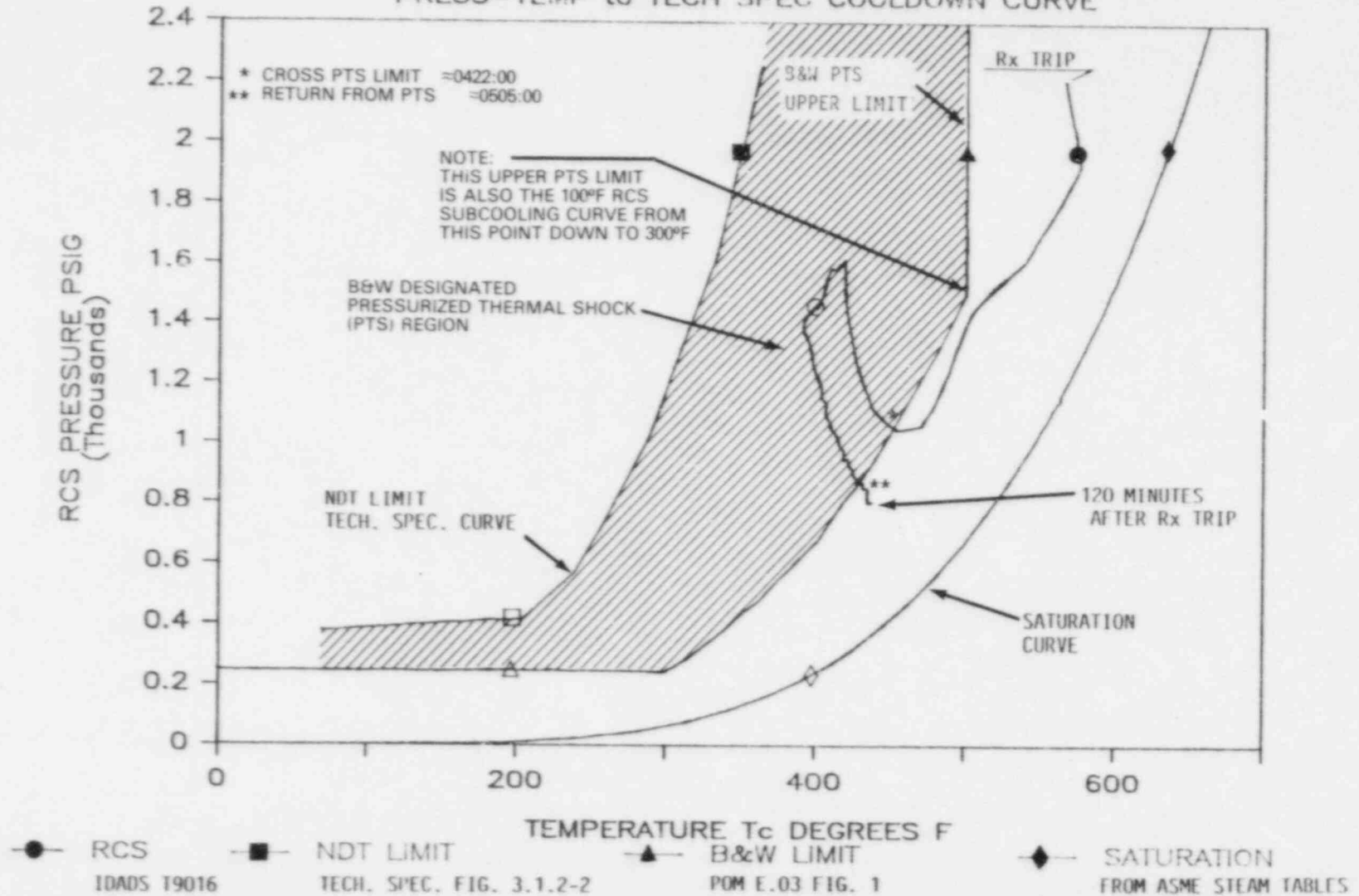


Figure 4.6 Comparison of reactor pressure-temperature with B&W PTS and NDT Technical Specification limits

## 5 EQUIPMENT PERFORMANCE

### 5.1 Integrated Control System

The December 26, 1985 overcooling transient at the Rancho Seco nuclear station was initiated by the complete loss of dc power within the integrated control system (ICS). Upon loss of its dc power, the ICS caused many control valves to go to the 50 percent open position. Since the plant was at 76 percent power when the ICS lost power, the 50 percent valve positions resulted in a significant reduction in feedwater flow. Although the open atmospheric dump valves (ADVs) and turbine bypass valves (TBVs) produced a significant steam flow, on balance, the result was undercooling of the reactor coolant system (RCS) and a reactor trip on high RCS pressure. After the nuclear heat source was tripped, the 50 percent open valve positions caused a substantial overcooling. The ICS power loss also affected several switching relays in the ICS which directly affected plant equipment in ways that were not recognized by the control room operators, e.g., shutting the main feedwater (MFW) stop valves. Finally, the loss of ICS dc power prevented operators from controlling equipment remotely from the control room that would have stabilized plant conditions. Operator performance associated with the ICS system is discussed in Section 6.7.

#### 5.1.1 Root Cause Determination

Sacramento Municipal Utility District (SMUD) developed a systematic troubleshooting plan (dated January 8, 1986) to ascertain the root cause of the loss of ICS dc power. Although this plan identified nine possible causes, a malfunction related to the power supply monitor was considered to be the most likely cause, since it is the only module that can cause switches S1 and S2 to go to the OFF position.

The troubleshooting plan also investigated the equipment response upon loss of ICS dc power and upon restoration of power after about 26 minutes, as occurred during the incident.

The results of this troubleshooting are as follows:

1. The +/- 24 Vdc bus voltages and the output contacts of the power supply monitor were monitored continuously on a strip chart recorder for over 30 days after the incident to record any intermittent actions. None occurred.
2. The visual inspection of the equipment revealed no significant abnormal condition.
3. The setpoints for that portion of the power supply monitor that monitors the output voltages of the individual power supplies were all found to be normal. The auctioneering diodes were shown to be functioning properly. The troubleshooting did reveal a minor discrepancy between the drawings and the actual wiring. Even so, this discrepancy did not affect the operation of the power supplies or the power supply monitor, and did not contribute to the loss of power.



4. The load-carrying capability of the power supplies was verified and they were shown to be capable of picking up the full load instantly without tripping the power supply monitor.
5. The troubleshooting revealed voltage and current spiking on the +/- 24 Vdc ICS buses when the circuit breaker to the ICS from vital 120 Vac bus 1C was tripped during the test. The voltage spikes were 1 volt or less in magnitude and were shorter than 1/100 second in duration. The bus load current spiked to about 16 Amps and dropped to about 7 Amps from the nominal load of 10-11 Amps. The spiking was greater on the positive bus than on the negative bus. The voltage spiking was not of sufficient magnitude or duration to actuate the power supply monitor or the overvoltage (i.e., crowbar) protection within the individual power supplies. The current spiking may have actuated the current-limiting feature of the power supply, which is set at 15 Amps. Since the ac circuit breaker from the vital bus did not trip during the incident, the spiking is not considered to be a cause of the loss of ICS dc power during the December 26, 1985 incident.
6. When the setpoints for the portions of the power supply monitor that monitors the bus voltages were checked, some unexpected effects were observed. The -24 Vdc portion worked properly. When the voltage was lowered, the power supply monitor tripped at -22.0 Vdc (the expected value) and the power supply monitor demonstrated a distinct deadband (hysteresis) between the trip and reset values of 0.09 Vdc (as compared to the expected value of 0.08 Vdc). However, when the voltage was lowered on the positive bus, the power supply monitor tripped prematurely at 22.5 Vdc. As the voltage was raised and lowered, it was impossible to identify a specific setpoint value. When the voltage was held constant at any value between 22.5 and 22.8 Vdc, the power supply monitor tripped and reset intermittently. Further investigation into this unusual and erratic behavior revealed a 1-volt drop between the +24 Vdc bus and the input to the power supply monitor (an unexpectedly large value) and a 2-ohm resistance (also unexpectedly large). The resistance value was noted to be changing with time. When a jumper was installed temporarily between the bus and the power supply monitor, the performance of the power supply monitor was improved but still not proper.

Two causes for the erratic behavior of the power supply monitor were identified. First, the design of the power supply monitor was shown by bench testing to be extremely susceptible to voltage/resistance changes at its input. The voltage being monitored also supplies the power used to operate the module and the current required for the module decreases significantly when the module changes from the untripped state to the tripped state. For various values of simulated "contact resistance" between the bus and the power supply monitor, the module either does not trip, acts erratically, works properly, or is continuously tripped. Second, a factory-installed wiring connection (i.e., crimp) at the +24 Vdc wiring in ICS cabinet No. 1 was found to have caused the high resistance.

During this test, technicians noted that when the bus voltage is 21.8 Vdc (i.e., slightly below the specified minimum allowed voltage of 22.0 Vdc), the transfer relays cycled on and off erratically at an interval of about 1 second. The ICS was not expected to perform properly at this supply voltage.

7. The time delays associated with the automatic tripping of switches S1 and S2 were found to be only 0.144 and 0.129 seconds, respectively, which is significantly less than the expected value of 0.500 seconds. The shortened delay would make the system more susceptible to spurious losses of power and may complicate the restoration of ICS power.
8. Video cameras in the control room were used to monitor the changes of indicators and demand values as ICS dc power was turned off and later restored. When power was interrupted, all the ICS demand signals went to 50 percent except the MFW pump speed demand, which went to zero demand. Unexpectedly, the control station for the plant auxiliary steam system was also affected by ICS dc power and was de-energized. The only indicators affected were the recorders for MFW flow (the MFW flow meters were not affected) and the frequency indicator for the main generator, both of which went to the mid-scale positions. The behavior of the MFW flow recorder may have been expected by some members of the plant technical staff, but was not expected by the control room operators. The behavior of the frequency indicator was unexpected by everyone.

Subsequently, a review of the plant drawings indicated that these unexpected responses were by design and should have been expected. The MFW flow recorder and the control station for the auxiliary steam system are actually powered by the ICS dc power. The generator frequency meter actually displays the ICS frequency error signal, although the meter is labelled "generator frequency."

The loss of power to the flow recorder and steam control station caused each to go to their mid-scale values. This incorrect indication on the flow recorder contributed to the control room operators belief that there was significant MFW flow, when there actually was none. The demand signal for the pressure for the auxiliary steam went to 50 percent. This occurrence had no affect on this particular plant transient. The mislabeling of the generator frequency meter is considered to be a human factors concern that had no affect on this particular plant transient. The most significant aspect of these three discoveries is that, in spite of all the concerns raised in recent years, the plant operating staff was unaware that these indicators were dependent upon ICS power.

9. The results upon re-energization during the test were unexpected also. During the testing, not all the initial demand signals for the key ICS-controlled valves were 100 percent, as had been reported during the incident. The test was repeated twice with the same results; however, as discussed further below, not only did the hand/auto stations energize to different initial demand values, but then some demand values began to change with time. Generally, the initial demand valves were either 100 or 0 percent. The differences are interesting. The demand signal for the TBVs went to 0 percent demand, while the demand for the ADVs went to 100 percent. Also, there were differences between trains for corresponding equipment. For example, the demand for the A AFW (ICS) flow control valve went to 100 percent, while the demand for the B AFW (ICS) flow control valve went to 0 percent. The apparent discrepancy between the results of this test and the results reported by the operators for the incident has not been fully explained. After the initial demand signals occurred, some demands changed value. For example, the initial reactor power demand was 100 percent and then it decreased to 0 percent within about 3 seconds.

The initial demands for both MFW pump speeds were 100 percent and then they decreased to 50 percent in 31 seconds and further decreased to 0 percent in the next 25 seconds. It was noted also that some ICS-related annunciators which had been on prior to the power interruption, went off when the power went off. When power was restored, different ICS-related annunciators (e.g., OTSG A Low Level Limit) came on.

10. Inspection and testing of the power supply monitor on the bench revealed that several of the operational amplifiers had been replaced previously and that there was an intermittent failure in the module. This intermittent failure seems to prevent the power supply monitor from tripping switches S1 and S2. Since this consequence is the direct opposite of what occurred on December 26, 1985, this intermittent failure does not appear to be related to this incident.

SMUD prepared an engineering report which provides the details of the troubleshooting and the technical justification for the root cause determination.

After reviewing the engineering report, the Team concludes that the December 26, 1985 overcooling transient was initiated by the failure of a single module in the nonsafety-related ICS (i.e., the spurious tripping of the power supply monitor module). The most probable cause of this failure is (1) a design weakness related to the power supply monitor that makes it susceptible to erratic operation (item 6 above); and (2) the development of a high-resistance electrical wiring connection that exposed the design weakness (item 6 above). This situation may have been aggravated by the shorter-than-normal time delay associated with switches S1 and S2, which would have made the ICS power distribution system more susceptible to electrical transient effects (item 7 above).

A significant uncertainty remains in establishing the root cause of the failure precisely. For example, no analysis of the circuit design has been performed to define the design weakness and establish this weakness as the root cause. The intermittent failure in the module is not well defined and whether or not there is any interaction between this failure and the design weakness is not known. Further, other factors have been identified by the Team as, at least, potential contributors to the failure. The Team did conclude that the cause has been isolated to the combination of the the power supply monitor and switches S1 and S2. On the basis that SMUD agreed to identify the cause of the failure by having an independent laboratory conduct appropriate circuit analysis, failure analyses, and testing of these components, the Team removed the remainder of the ICS from the quarantine list.

The Team also concludes, based upon the unexpected nature of the troubleshooting results discussed above, that the effects of loss of ICS dc power were not well understood by the control room operators prior to the incident. Further, the ICS performance upon restoration of power was not known prior to the incident and is still not understood. Due to the potentially generic applicability of this matter, the Team has agreed with the SMUD decision to reduce the scope of the troubleshooting action plan at Rancho Seco because the B&W Owner's Group will investigate this matter.

## 5.2 AFW (ICS) Flow Control Valves

The loss of ICS dc power caused the AFW (ICS) flow control valves (FV-20527 and FV-20528) to travel from the fully closed position to the 50 percent stroke

position. The motor-driven AFW pump and the dual-drive AFW pump started 14 and 19 seconds, respectively, after the loss of dc power because of the associated loss of MFW. This resulted in feeding cold auxiliary feedwater from the condensate storage tank to the once-through steam generators (OTSGs).

The Control Room Operators diagnosed that they had lost automatic and remote (CR) control of the AFW (ICS) flow control valves. They also realized that they were experiencing a rapid cooldown transient. Therefore, nonlicensed operators were dispatched to shut the valves locally, using the manual handwheels attached to the diaphragm actuators. It is important to note that these valves are located outdoors, and at the time of the event (4:00 a.m.), it was cold, dark and very foggy.

The nonlicensed operator arrived at the B AFW (ICS) flow control valve (which feeds the B OTSG) and turned the manual handwheel in the closed direction until resistance was encountered. Assuming the valve was shut, he proceeded to the A AFW (ICS) flow control valve (which feeds the A OTSG). Subsequent review of AFW flow data indicates that flow to the B OTSG dropped by only about 40 percent at this time.

When attempting to close the A AFW (ICS) flow control valve, the operator encountered more resistance. The AFW system configuration may have contributed to this difficulty. The pump discharges are cross-tied through HV-31826 and HV-31827 (See Figure 3.8). Thus, closing the AFW flow control valve to one OTSG apparently shifted much of the flow to the other OTSG line. Therefore, the increased flow might have contributed to his difficulty in closing the A AFW (ICS) flow control valve compared with the B AFW (ICS) flow control valve, although the valves are designed to be flow balanced. The reason for this difficulty has not been determined.

After working for several minutes, the nonlicensed operator checked the valve stem on the A AFW (ICS) flow control valve and noted that about 1/2 inch of uncorroded stem was visible (the full stroke of this valve is 2 inches). He assumed that this meant that the valve was still partially open, and left the area to obtain a valve wrench to help him close the valve completely. When he returned and applied the valve wrench to close the valve further, the manual operating mechanism broke loose from the actuator and spring pressure reopened the valve.

The operator reported the problem to the control room and was directed to close the manual isolation valve (FWS-063) downstream of the A AFW (ICS) flow control valve. However, he was unable to move the manual isolation valve from its open position even with the aid of a valve wrench (cheater). (See Section 5.3 for more details on this failure.)

In the meantime, a second nonlicensed operator arrived at the B AFW (ICS) flow control valve. He was unaware that the first operator had already attempted to close the valve. The second operator completely closed the B AFW (ICS) flow control valve with the manual handwheel, thereby stopping AFW flow to the B OTSG. This occurred about 20 minutes after the initial loss of ICS power.

Before the operators could take any additional actions, electrical power was restored to the ICS. The A AFW (ICS) flow control valve was then closed from

the control room to stop AFW flow to the A OTSG about 26 minutes after the initial loss of ICS power. (Personnel performance associated with the AFW (ICS) flow control valve is discussed in Section 6.8.)

### 5.2.1 Component Description

AFW (ICS) flow control valves, are direct-acting, spring-opposed, and air-actuated (See Figure 5.1). SMUD representatives have stated that the entire AFW system is safety related. However, it is obvious that these valves are not fully safety related because they are controlled by the nonsafety-related ICS. The valves use a Fisher diaphragm actuator and have a valve stroke of 2 inches. Air is supplied to the top of the diaphragm. A travel indicator is attached to the valve stem and a travel indicator scale is mounted on the valve actuator yoke (see Figures 6.2 and 6.3). The indicator consists of two horizontal discs attached to the valve stem by a nut and a jam nut. The indicator scale is graduated vertically, with an arrow pointing upward to the open position. The closed position is not specifically labeled on the scale. However, the bottom mark on the scale corresponds to the closed position.

The valves are furnished with a side-mounted handwheel assembly (see Figures 5.2 and 5.3). The handwheel assembly is attached to the actuator yoke by a U-bolt and two J-bolts. A lever and pin assembly couples the handwheel to the valve stem. Two dowel pins are provided to ensure the handwheel is properly positioned on the yoke. A "neutral" position indicator is provided, indicating the handwheel position at which automatic operation of the valve is possible over full range of valve travel. When the handwheel is positioned at any other point than "neutral," automatic full travel will be restricted in one direction.

### 5.2.2 Root Cause Determination

SMUD developed a systematic troubleshooting plan (dated January 7, 1986) to identify the root cause of the failure of the A AFW (ICS) flow control valve. Although the B AFW (ICS) flow control valve did not fail during the event, the scope of the troubleshooting was expanded to include that valve, since it is the same type and serves the same function as the A AFW (ICS) flow control valve.

The plan identified several possible primary and contributing causes for why the manual handwheel mechanism broke loose from the valve actuator:

1. Excessive force on the handjacking mechanism
2. Improper mounting bolt torque
3. Improper positioning of the handjacking mechanism on the actuator yoke
4. Inadequate operator training
5. Lack of adequate area lighting, preventing the operator from seeing the position indicator
6. Inadequate valve stem position indication method
7. Inaccessability of the valve position indicator.

The results of the troubleshooting are described below.

A review of the "as-found" conditions of the A AFW (ICS) flow control valve revealed that excessive force had been applied to the handwheel assembly. This finding was substantiated by the following indications:

- o The two dowel pins (Figure 5.3) were found sheared and lying below the valve operator. There was no indication of fatigue-induced failure of the pins.
- o The dowel pin holes in the actuator were elongated.
- o The lever pivot pin was bent.
- o Cracks were found in the bushing and in the handwheel assembly casting.

After the dowel pins sheared, the handwheel assembly broke free from the operator yoke (Figure 5.4).

The handwheel assembly was also found to be improperly mounted on the valve actuator yoke. Thus, improper mounting forced the dowel pins to assume the load being transmitted by the handwheel. Mounting discrepancies included the following:

- o The lower U-bolt had been replaced with two J-bolts.
- o The nuts attaching the J-bolts to the valve operator were both loose.

There were also indications (chipped paint) that the operating nut had previously bottomed out against the housing in the closed position. This condition may indicate that the handwheel setting was left in other than the "neutral" position, thereby restricting motion in the closed direction while the valve was operated in automatic. It appears that positioning the handwheel exactly to the neutral position is crucial for this type valve.

Inspection of the B AFW (ICS) flow control valve provided several similar indications that excessive force had been applied from the handwheel assembly. Moreover, the damage indicated that excessive force had been applied prior to the December 26, 1985 incident. There were also indications that the handwheel assembly had previously moved on the actuator. The J-bolts on the B AFW (ICS) flow control valve were also found to be loose.

The prior damage to the valves may have contributed to the difficulty that the operators encountered in shutting the AFW (ICS) flow control valves. This difficulty may have prompted the operators to use a cheater and apply excessive force to the valve.

### 5.3 AFW Manual Isolation Valve

Following his unsuccessful attempts to close the A AFW (ICS) flow control valve, the nonlicensed operator was directed to close the manual isolation valve (FWS-063) downstream of the A AFW (ICS) flow control valve. However, these efforts were unsuccessful, despite the use of a large valve wrench, and the valve remained fully open.

#### 5.3.1 Component Description

The manual isolation valve is a locked-open valve located in the AFW discharge header to the A OTSG. A SMUD representative has stated that the entire AFW system, which would include this manual isolation valve, is safety-related.

However, from other discussions with SMUD personnel, it appears that this valve was only intended to be used to isolate the AFW (ICS) flow control valve for maintenance. The valve is a 6-inch, ANSI Class 900-lb, pressure seal gate manufactured by Velan Engineering. It is categorized as an ASME "Category E" valve (i.e., it is normally locked open to fulfill its function).

It has a rising stem handwheel and is provided with a stellite-faced positive backseat, integral with the valve bonnet (see Figure 5.5).

The valve handwheel is attached to a yoke nut, which turns with the handwheel. Turning the yoke nut results in vertical movement of the stem. Vertical yoke nut movement is restricted by the yoke nut housing and an upper and lower bearing. The yoke nut assembly is designed to be lubricated through a grease fitting (Figure 5.5). Forcing grease into the yoke nut assembly lubricates the upper bearing, lower bearing, yoke nut, and stem threads.

The Velan instruction manual (VEL-PS-3) provides the following guidance regarding maintenance and operation of the valve:

- o Lubrication of the stem threads and other working components should be performed frequently and at least every 6 months. A lubrication schedule recommends stem thread lubrication whenever the threads appear dry, and greasing of the yoke sleeve bearings concurrently with stem thread lubrication.
- o Valves that are not operated frequently and may remain open or closed for long periods of time should be worked, even if only partially, about once a month.
- o Proper lubrication of the stem and sleeve can reduce required operating torque by 7 to 30 percent.
- o A caution is also provided not to use valve wrenches on the handwheels.

Section XI of the ASME Boiler and Pressure Vessel Code requires no regular testing of Category E valves. The positions of the valves are merely recorded to verify that each valve is locked or sealed in its correct position.

### 5.3.2 Root Cause Determination

SMUD developed a systematic troubleshooting plan (dated January 4, 1986) to identify the root cause of why the manual isolation valve could not be closed. As part of that plan, the maintenance history of the manual isolation valve and five other similar valves in the AFW system was reviewed. The five other valves were as follows:

FWS-064	AFW to B OTSG Manual Isolation Valve
FWS-053	A AFW Pump Discharge Isolation Valve
FWS-054	B AFW Pump Discharge Isolation Valve
FWS-119	AFW from B AFW Pump Isolation Valve to B OTSG
FWS-120	AFW from A AFW Pump Isolation Valve to A OTSG

A review of the maintenance history of FWS-063 indicated that no maintenance (preventive or corrective) has been performed on the valve during the operational life of the plant (i.e., since 1974).

Two of the similar valves had failed previously, which prevented movement of the valve from the open position. The discharge isolation valve from the A AFW pump failed on November 20, 1979 and the AFW manual isolation valve to the B OTSG failed on February 20, 1980. In both cases, the yoke bearings (Figure 5.5) were found seized and had to be replaced.

The troubleshooting plan identified several possible causes for the failure of manual isolation valve to the A OTSG:

1. Failed yoke nut bearing.
2. Overtightening of the valve packing.
3. Misaligned packing gland follower causing binding on the stem.
4. Damaged or bent valve stem or other damaged valve internals.

The results of the troubleshooting are described below.

An inspection of the "as-found" condition of FWS-063 indicated that the yoke nut assembly had seized. Both the upper and lower yoke nut bearings were extensively rusted and pitted, and there was no evidence of any lubrication. (See Figure 5.6).

The yoke nut assembly was cleaned and lubricated, the bearings were replaced, and the valve was reassembled. Following these repairs, FWS-063 operated smoothly with little force required on the handwheel.

The Team concluded that the root cause of the failure was inadequate lubrication, which led to the yoke nut seizing. Since the valve operated smoothly following reassembly, the other potential causes for failure were discounted.

The five other similar valves were inspected and all operated satisfactorily. However, there was no evidence of recent lubrication on any of the valves.

#### 5.4 Makeup Pump

When the ICS power was lost, the makeup system was in its normal alignment with the makeup pump (P-236) taking water from the makeup tank (MUT) and discharging to the RCP seals and to the normal makeup line through makeup valve SFV-23604. (See Figure 3.12). The suction isolation valves between the makeup pump and the A HPI pump were open, while those between the makeup pump and the B HPI pump were closed.

Following the loss of ICS power, reactor trip, and AFW initiation, the operators noted that the pressurizer level was decreasing, so they opened the A HPI injection valve (SFV-23811) fully to increase makeup flow to the RCS. The suction valve from the BWST (SFV-25003) to the makeup pump and to the A HPI pump was then opened. The B HPI pump was subsequently started, taking its suction from the BWST (SFV-25004).



About 3 minutes into the transient, RCS pressure had decreased to 1600 psig and an SFAS initiation resulted. The following actions (in the makeup/HPI system) resulted from that initiation:

1. HPI loop injection valves (SFV-23809, SFV-23810, SFV-23812) opened. Note that one HPI loop injection valve (SFV-23811) had previously been opened by the operator.
2. The suction valves from the BWST (SFV-25003 and SFV-25004) received an "open" signal, though both were already open.
3. The suction valve from the MUT (SFV-23508) closed. The suction valve from the MUT shuts on SFAS actuation to prevent normal makeup water from diluting the HPI flow from the BWST, and to prevent gas binding of the HPI pumps if the MUT were to empty.
4. The recirculation valves (SFV-23645 and SFV-23646) from the A HPI pump and the makeup pump discharge lines to the MUT closed.
5. The normal makeup valve (SFV-23604) closed.
6. The A HPI pump (P-238A) started.

At this point, all three pumps were running, taking water from the BWST and injecting through the HPI lines (and to the RCP seals).

About 5 minutes after the SFAS initiation, the operator had an indication that RCS pressure was increasing. He then started to throttle back on HPI flow. About 3 minutes later, the recirculation valves to the MUT from the makeup pump and the A HPI pump (SFV-23645 and SFV-23646) were reopened to allow subsequent additional throttling of HPI flow (to control repressurization), while avoiding pump damage due to internal overheating. However, since the suction valve from the MUT (SFV-23508) had closed, opening these recirculation valves resulted in the MUT overflowing. The MUT relief valve then lifted and discharged water to the flash tank which subsequently overflowed to the waste gas storage tank.

Shortly after this, the operator stopped the A HPI pump and closed the D and C injection valves (SFV-23810 and SFV-23812). In an attempt to mitigate the high level in the MUT, the operator closed the suction valve from the BWST to try to draw more water from the MUT. He had overlooked the fact that the suction valve from the MUT (SFV-23508) had closed on SFAS initiation. Closing the suction from the BWST thereby isolated the suction to the running makeup pump.

Approximately 10 minutes later, the operator stopped the B HPI pump. He quickly noticed a loss of RCP seal flow and restarted the pump. (Note: The loss of RCP seal flow resulted from a failure of the makeup pump, although the operators were not yet aware of the problem.) During the next 6 minutes, the B HPI pump was stopped again and restarted since seal flow again decreased. Coincident with this seal flow problem, the auxiliary building stack radiation monitor alarmed.

During this period, the operators in the control room heard a loud noise, observed that the makeup pump meter was indicating only about 1/3 of its normal

running current, and realized that the makeup pump had been damaged (see Figures 5.7 and 5.8). About that time, they also noted that the suction valve from the MUT to the makeup pump was closed. The operators immediately stopped the pump and opened the valve, thinking that this might somehow reduce the damage to the pump. However, MUT level began dropping rapidly so the MUT outlet valve was closed.

The operators were then concerned that a potential leakage path from the RCS or from an operating HPI pump back through the makeup line might occur. In addition, a potential leakage path for releasing reactor coolant to the atmosphere existed through the common pump recirculation header. Thus, the operators appear to have been concerned that a small loss of coolant accident (LOCA) could develop if the pump was not isolated. Therefore, nonlicensed operators were dispatched to isolate the makeup pump by closing the manual isolation valves (SIM-001, SIM-003), and the minimum flow recirculation valve located in the pump room.

The operators donned available protective clothing, performed a brief radiation survey of the area (the reading was about 30 mrem/hr in the vicinity of the pump), and proceeded to isolate the pump. Water (mixed with oil) was about 4 inches deep around the pump and extensive damage was noted to the pump seals, bearings, bearing housing, and shaft. Upon leaving the area, both operators found that their clothing had become radioactively contaminated, so they disposed of it. (Personnel performance associated with operation of the makeup pump is described in Section 6.7.)

#### 5.4.1 Component Description

The makeup and HPI pumps, which are all safety related, are identical horizontally mounted, nine-stage, centrifugal pumps (See Figure 5.9). Each is rated for a normal discharge pressure of 2900 psig, with a flow rate of 300 gpm. A minimum net positive suction head (NPSH) of 30 feet is required to prevent the pumps from cavitating. An ac motor that turns at 1780 rpm is connected to each pump through a high speed gear drive, resulting in a pump speed of 6018 rpm.

These multi-stage pumps, operating at high pressure, generate a considerable amount of internal heat due to frictional losses. A minimum flow of 105 gpm is needed through the pumps (while in continuous operation) to avoid the potential pump damage from heat. The minimum flow can be reduced to 40 gpm, but only if the pump is operated less than 15 minutes. The maximum allowable pump operating time when flow is less than 40 gpm is 15 seconds. There is a minimum flow recirculation path installed to provide the necessary minimum flow.

#### 5.4.2 System Response and Interactions

The designed makeup system response to an SFAS initiation and subsequent recovery from the SFAS initiation contributed to failure of the makeup pump.

Maintaining minimum flow through the running pumps is necessary to prevent damage from overheating. At the same time, it is necessary to throttle back on injection flow during a cooldown to avoid excessive repressurization and entry into the pressurized thermal shock (PTS) region. The logical way to accomplish both of these tasks is to open the minimum flow recirculation line valves (SFV-23645 and SFV-23646) back to the MUT. However, since the MUT outlet is

isolated on an SFAS initiation, such action will normally result in the MUT overfilling.

In addition, having the minimum flow recirculation lines from all three pumps joined in a common header (upstream of the pump discharge check valves) contributed to the need to manually isolate the makeup pump after it failed. If the makeup pump (P-236) were not isolated manually, only a single stop-check valve separated the running B HPI pump and the makeup pump through the recirculation line.

### 5.5 Pressurizer

During the December 26, 1985 incident, pressurizer water level was off-scale low for a period of 10 minutes. This section discusses whether the pressurizer emptied completely and, if so, whether a bubble formed elsewhere in the RCS.

After the December 26, 1985 incident, SMUD performed an RCS mass balance to determine the pressurizer level during the time it was below the lower tap (04:16:40 to 04:26:20 a.m.). In addition, B&W did an independent but similar evaluation by calculating a net reactor coolant volume change from RCS temperatures and HPI flowrate.

The mass balance showed that the pressurizer emptied at approximately the same time that a sharp drop in RCS pressure began to occur at 04:19 a.m (see Figure 4.1). During this time, the surge line flow was steam which was condensing in the hot leg and/or OTSG.

A mass balance of the RCS indicates that just before the pressurizer emptied, coolant volume was contracting at a rate of 200 ft<sup>3</sup> per minute due to a cooldown rate of 18°F per minute. Approximately 2/3 of this was made up with HPI and 1/3 with pressurizer outsurge. Immediately after the pressurizer emptied, the high depressurization rate and the heating effect of the steam/water surging into the hot leg reduced the rate of contraction by about 20 percent. The steam that condensed in the coolant made up most of the rest of the volume. Steam formation in the vessel upper head probably accounted for a small volume. Shortly after the pressurizer emptied, the cooldown rate began to taper off and by 04:21:30 a.m. was down to 13°F per minute and HPI flow alone was able to keep up with the contraction rate of the coolant. At this point, pressure stopped decreasing at 1047 psig. Saturation pressure in the hot leg was 480 psi. As the cooldown rate continued to taper off, HPI flow exceeded the contraction rate and began to refill the pressurizer and raise pressure.

SMUD concluded that it is probable that some boiling occurred along thick metal walls in the reactor vessel head. The pre-trip hot leg temperature (and hence metal temperature) was 600°F, and the saturation temperature at the minimum RCS pressure was 550°F. Because the vessel design forces flow through the upper head, any steam that formed would tend to be condensed after a short time, and no large accumulation would occur. Also, no significant accumulation of steam would occur in the hot leg because the high flow rate and subcooling would have caused any steam to be condensed in the hot leg or carried into the OTSG and condensed.

The B&W calculation concluded that the pressurizer emptied and a small (less than 100 ft<sup>3</sup>) steam volume was formed elsewhere in the RCS.

In summary, the pressurizer and surge line completely emptied during the transient and a steam bubble probably formed in the reactor vessel head, a condition which helped maintain pressure. The RCS remained subcooled throughout the transient.

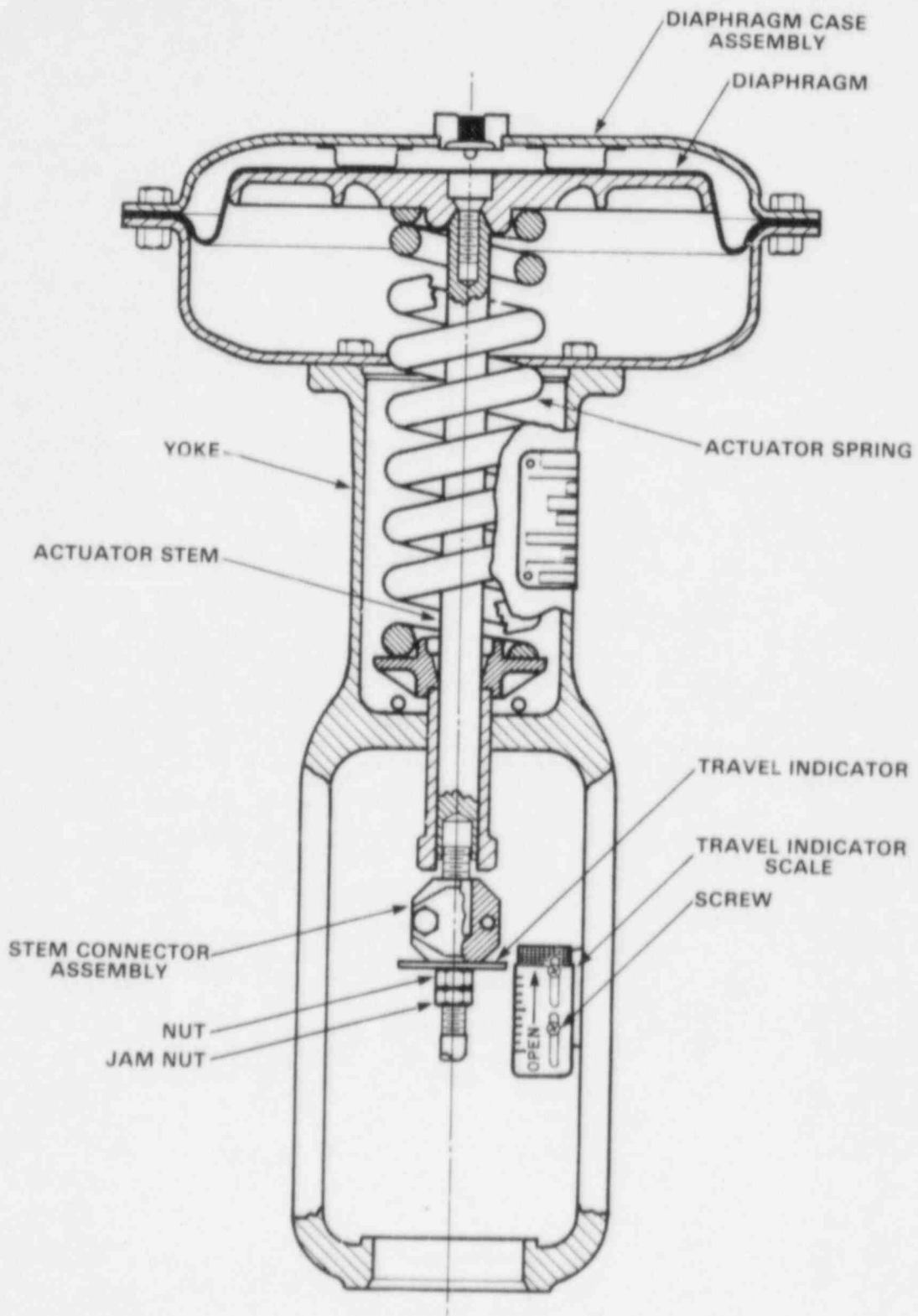


Figure 5.1 AFW(ICS) flow control valve

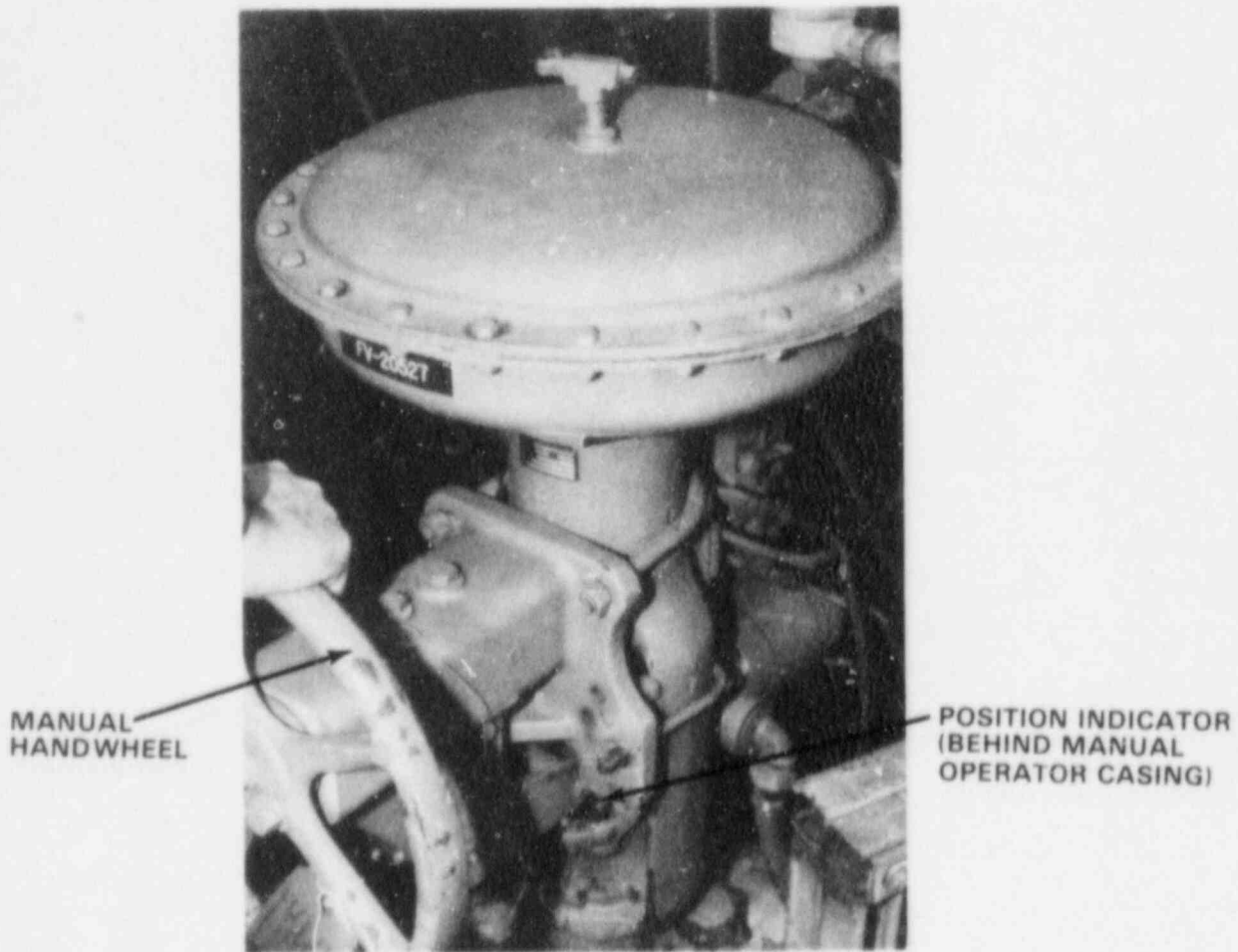


Figure 5.2 A AFW(ICS) flow control valve (FV-20527)

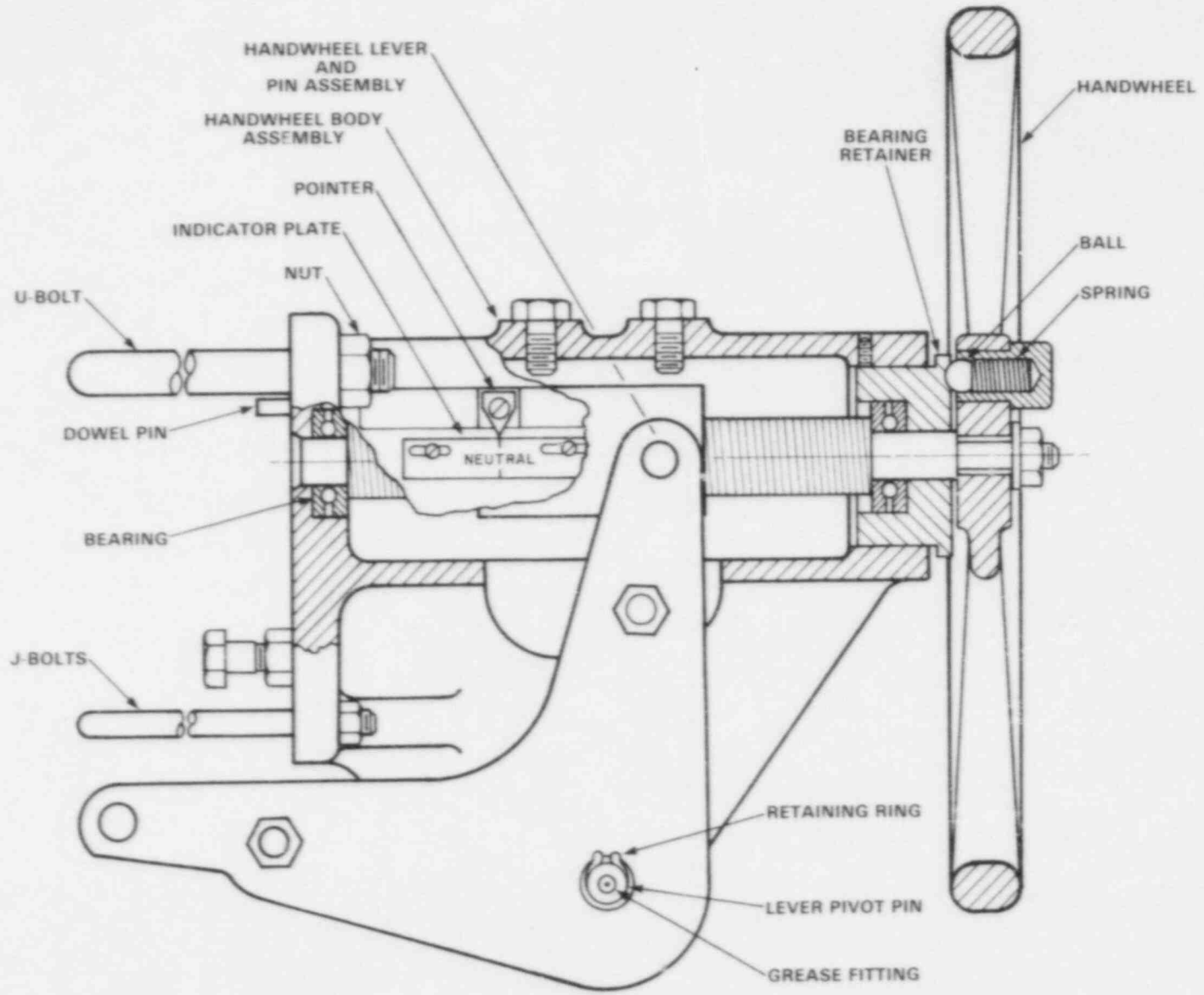


Figure 5.3 AFW(ICS) flow control valve manual operator

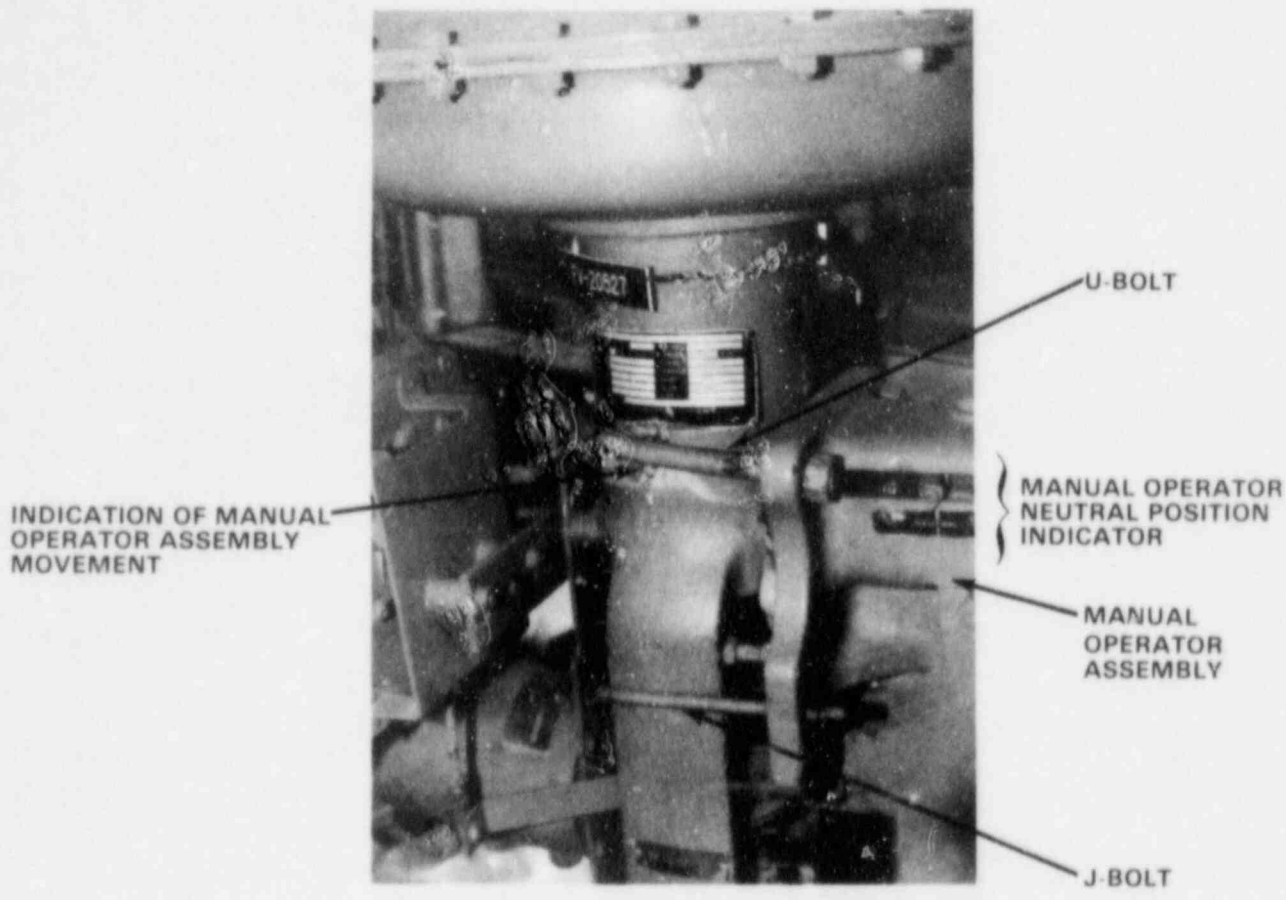


Figure 5.4 Damage to the A AFW(ICS) flow control valve



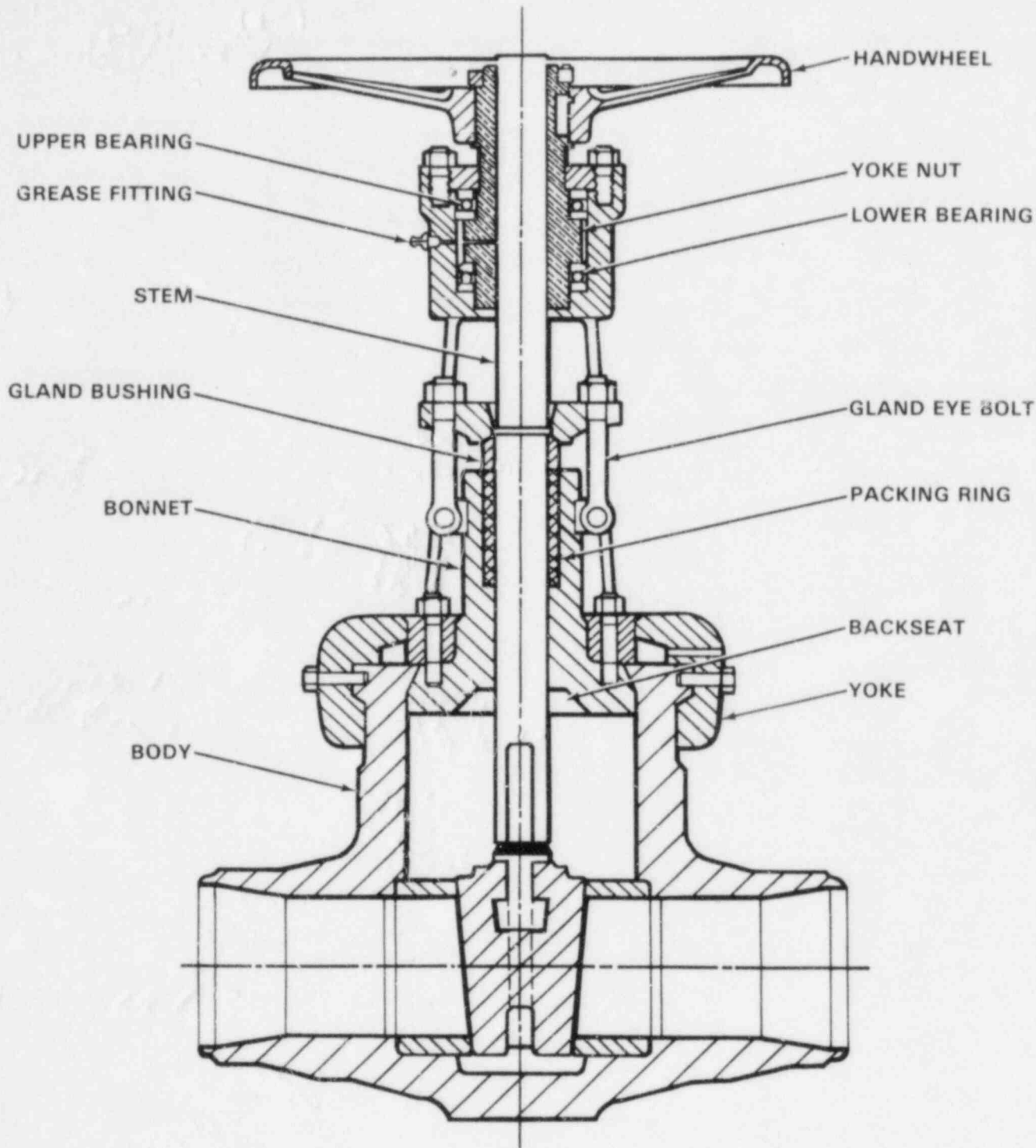
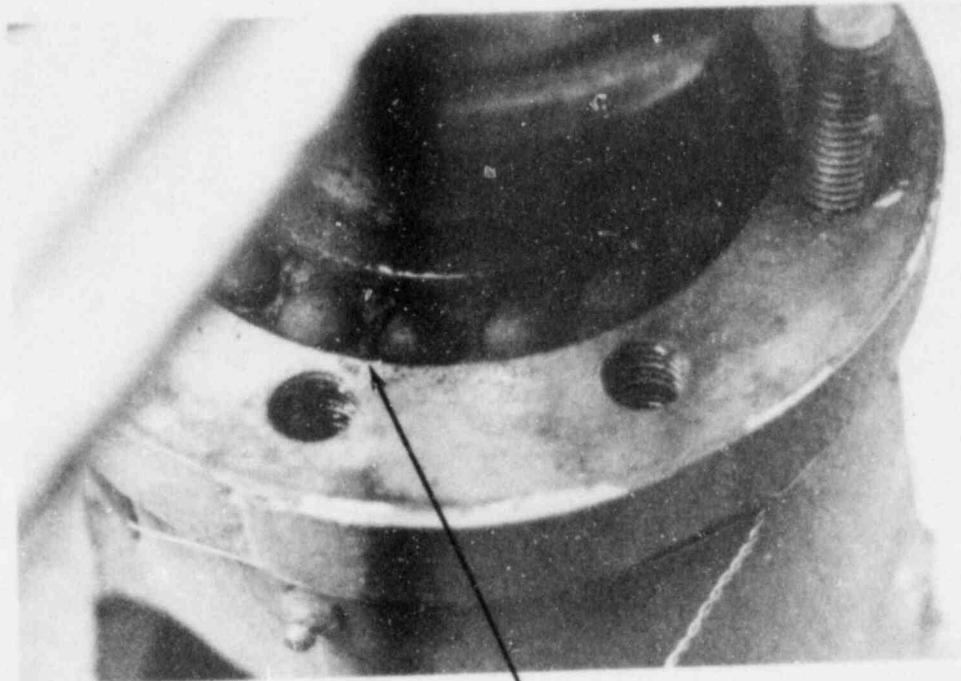


Figure 5.5 AFW manual isolation valve



UPPER BEARING

Figure 5.6 AFW manual isolation valve (FWS-063) upper bearing

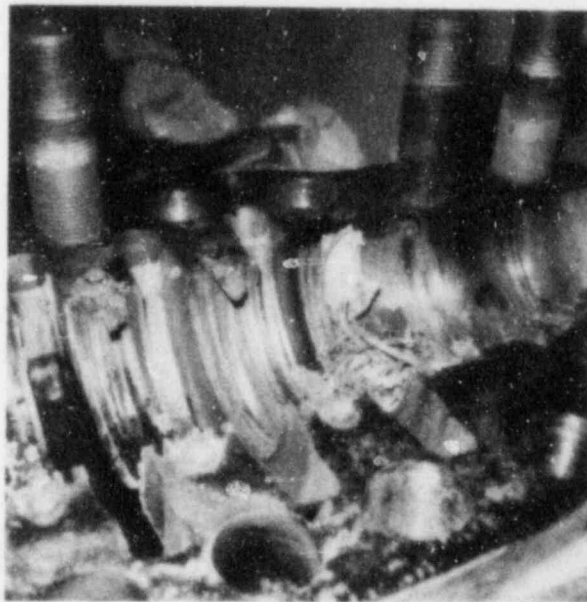


Figure 5.7 Makeup pump lower casing



Figure 5.8 Makeup pump impeller and wear rings

## 6 PERSONNEL PERFORMANCE

### 6.1 Introduction

This section assesses the response to the December 26, 1985 incident by Sacramento Municipal Utility District (SMUD) personnel and the human factors issues affecting their performance. Local, State and Federal authorities were notified of the event, but since these organizations did not play a significant role, their participation is not addressed in this report. The personnel who responded were members of the onshift operating crew. Although additional SMUD personnel were called, they did not arrive until after the plant was stabilized.

In addition to an evaluation of the response of the onshift crew to plant conditions, this section discusses the adequacy and degree of operator compliance with plant procedures. This section also briefly assesses the role of the Shift Technical Advisor (STA) and evaluates the training received by licensed and nonlicensed operators relative to their response to this event.

SMUD made their initial notification to the NRC of the December 26, 1985 incident at 4:32 a.m. Pacific Standard Time (PST) via the Emergency Notification System (ENS). Notification was made by the Senior Control Room Operator and included a declaration of an Unusual Event and a brief description of the transient. ENS communication between SMUD and the Nuclear Regulatory Commission (NRC) was then terminated for approximately one-half hour. ENS communications with SMUD were reactivated at about 5:00 a.m. PST and an open line was maintained until the Unusual Event was terminated. At the time communications were re-established, integrated control system (ICS) dc power had been restored, and the operators had terminated the plant cooldown. The Team reviewed the transcript of these conversations. No significant problems were encountered with the ENS, and communications between SMUD and NRC, for the most part, accurately characterized the incident. Thus, the Team concluded that the ENS functioned as intended as a communication channel between SMUD and NRC.

### 6.2 Shift Staffing

SMUD's response to this event was made by the onshift operating crew comprised of four Senior Reactor Operators (SRO), one of whom was the Shift Technical Advisor (STA); two Reactor Operators (RO); and six nonlicensed operators. Twelve operators were available onsite when the event began. (Four additional operators who would normally have been on shift were absent during the event because of Christmas vacations.) The plant's Technical Specifications and other SMUD regulatory commitments required that only seven operators be onshift during power operations (i.e., two Senior Reactor Operators, two Reactor Operators, two Nonlicensed Operators, and one Shift Technical Advisor). Therefore, the shift crew on duty during this event included five operators more than the minimum required.

.

Shift Crew on Duty

<u>Number</u>	<u>Position</u>	<u>License</u>
1	Shift Supervisor	Senior Reactor Operator
1	Backup Shift Supervisor*	Senior Reactor Operator
1	Shift Technical Advisor	Senior Reactor Operator
1	Senior Control Room Operator	Senior Reactor Operator
2	Control Room Operator	Reactor Operator
1	Auxiliary Operator	--
1	Equipment Attendant	--
1	Power Plant Helper	--
3	Auxiliary Operator Trainee**	--

During this event, operators initially took action to isolate eight valves at four different locations in the plant: two auxiliary feedwater (AFW) (ICS) flow control valves, four turbine bypass valves (TBVs), and two atmospheric dump valves (ADVs). Isolating these valves, which began within minutes of the loss of power to the ICS, had not been entirely completed when ICS dc power was restored 26 minutes later. The exertion required by these activities, and adverse weather conditions, may have contributed to the collapse of one Senior Reactor Operator in the control room.

The additional staffing, above that required by the Technical Specifications and other SMUD commitments was a significant factor in permitting a number of tasks to be performed simultaneously. With staffing at required levels, these tasks would have been performed sequentially, would have required longer to complete, and could have exacerbated the overcooling transient. In fact, even with the staffing available, the operators did not isolate AFW flow to the A once-through steam generator (OTSG) and, therefore, did not gain complete control of the plant cooldown transient before dc power within the ICS was restored.

---

\*An additional Shift Supervisor was assigned to this shift until the assigned Shift Supervisor, who was newly qualified, gained additional experience.

\*\*The Auxiliary Operator Trainees were all qualified as either Equipment Attendants (EAs) and/or Power Plant Helpers (PPHs) and functioned in those positions during the event.

### 6.3 Event Recognition

On loss of ICS dc power, several annunciator alarms actuated on the annunciator panels in the control room. The "ICS or Fan Power Failure" and several other alarms indicated that a perturbation had occurred in the ICS that in turn was affecting the entire plant. Most notable to the operators among those alarms was "ICS Runback or Limit." This alarm normally indicates that the ICS is automatically reducing plant power. (However, because of the loss of ICS power, the ICS was not actually reducing plant power.) When this alarm sounded, one of the control room operators immediately went to the ICS control station and the Shift Supervisor went to the reactor coolant system (RCS) pressure control station.

Thus, operators quickly recognized that there was a problem but it is not clear that they understood the source of the problem. The Shift Supervisor attempted to take control of reactor coolant system (RCS) pressure, which was rapidly increasing. He initiated pressurizer spray to decrease RCS pressure to prevent a reactor trip. However, he realized that the reactor was going to trip (which it did approximately 16 seconds after the ICS dc power was lost) before he got the spray valve fully open. After the reactor trip, he closed the spray valve.

Accompanying the high pressure trip of the reactor was noise caused by OTSG code safety valves relieving and the ADVs and TBVs opening. Soon after the reactor tripped, a Control Room Operator realized that he could not control the ICS-controlled valves remotely from the control room. In evaluating the instrumentation available to them, the Control Room Operators believed, incorrectly, that they were feeding the steam generators with main feedwater (MFW). Based on the fact that they had uncontrolled steam release and excess feed to the OTSGs, the operators realized that they were in an overcooling transient. Even at this point, it appears that they still did not realize that they had lost ICS power.

The Senior Control Room Operator, who had been on a plant tour at the time the incident occurred, quickly returned to the control room, arriving there prior to the tripping of the MFW pumps. Immediately after they tripped the MFW pumps, one of the control room operators noted that he did not have any power at the ICS control stations and announced to those in the control room that they had lost ICS power. At this point, approximately 2 minutes after the initiation of the transient, the operators realized that they had lost ICS power. The Shift Supervisor got the keys to unlock the ICS cabinets adjacent to the control room and three of the operators went to investigate the cause of the power loss.

In summary, it appears that the transient initiator (i.e., the loss of ICS dc power) was not fully recognized by the control room personnel until about 2 minutes after the power was lost. Although an annunciator alarm alerts operators about ICS power failures, it appears that the importance of the "ICS or Fan Power Failure" alarm was somewhat obscured 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.

Consequently, the operators did not immediately realize that the loss of ICS dc power was the transient initiator, and they responded to the symptoms of the

loss of power (e.g., an apparent plant "runback" and increasing RCS system pressure, which caused the subsequent reactor trip).

#### 6.4 Adequacy of Procedures

The procedural guidance available to the operators in the control room consisted of symptom-based Emergency Operating Procedures (EOPs). The EOPs are based upon the plant-specific Abnormal Transient Operating Guides (ATOG), which were prepared by the Babcock & Wilcox (B&W) Owners Group. The ATOG procedures are intended to be used as guidelines in developing plant-specific EOPs to mitigate transient conditions. Operators used three EOPs during this event. The first, E.01, "Immediate Actions," was completed by the Control Room Operator immediately upon trip of the reactor. There are four steps in this procedure, as follows:

##### E.01 Immediate Actions

Determine whether this is a reactor trip or a forced shutdown situation and proceed below:

<u>Reactor Trip</u>	<u>Forced Shutdown</u>
1. Manually trip the reactor.	1. <u>IF</u> a tube rupture/leak has occurred indicated by main steam line on air ejector off-gas or gland steam radiation monitor alarms, <u>THEN</u> go to SGTR E.06.
2. Manually trip the turbine.	2. <u>IF</u> a forced shutdown is required by Technical Specifications or by other operating documents, shutdown plant to required conditions per normal procedures, starting with OP B.4. Plant Shutdown and Cooldown.
3. Reduce letdown to 40 gpm.	
4. Immediately continue with E.02.	

The second EOP, E.02, "Vital Systems Status Verification," is intended to be used by the operators to assess the current condition of the plant and to direct them ultimately to an EOP that would deal with the incident based upon the symptoms they have identified. It is not clear whether the operators completed all 19 steps of E.02 on December 26, 1985. When the Senior Control Room Operator returned to the control room approximately 2 minutes after the reactor trip, he was handed the EOPs to direct the actions of the reactor operators and told that E.02 had been completed. Therefore, he did not use E.02 to assess the situation. Instead, he realized that an overcooling event was occurring and went directly to Procedure E.05, "Excessive Heat Transfer."

E.02 requires the verification of a number of specified conditions and then requires specific actions if a condition cannot be verified. The Team review



of E.02 indicates that the operators should have been able to verify all of the conditions until they reached Step 17, which would have directed them to Procedure E.05. Although E.02 is not a prerequisite that operators must complete before going to Procedure E.05, if conditions warrant, E.02 should be completed to verify system status and it should continue to be reviewed during an incident as a method of maintaining continual system surveillance.

E.05, which has 61 steps, is the appropriate EOP for the December 26, 1985 incident. However, it does not appear that operators completed more than the first three steps. To varying degrees the operators carried out the actions required by subsequent steps, although it appears that these actions were taken based on operator training and not on the faithful execution of the procedure.

Step 2 of E.05 refers to a situation where only one OTSG is causing the cool-down; therefore, it is not applicable.

Steps 1 and 3 of E.05 state:

E.05 Excessive Heat Transfer

Operator Action

- |  |   |
|--|---|
| 1. Maintain Pressurizer level above 100" | 1. Maintain pressurizer level above 100".   |
|  | .1 Keep makeup to the minimum necessary.  |
|  | .2 IF pressurizer level is below 100" AND RCS pressure is decreasing THEN increase makeup as necessary. |
|  | .1 Open HPI valve loop A (SFV-23811).   |
|  | .2 Start HPI Pump P-238B (HPI Pump lined up to the BWST).   |
|  | .3 Throttle loop A HPI injection valve SFV-23811 as necessary to control pressurizer level.             |
|  | .4 IF pressurizer level cannot be maintained above 100" THEN initiate Full HPI (Rule 1 and 2).          |

[STEP 2 OMITTED HERE]

---

Overcooling is Occurring from an Unidentified OTSG

---

\*\*\*\*\*  
 \* Caution \*  
 \* Shutting main steam to aux steam HV-20560 and HV-20565 \*  
 \* causes you to lose the air ejectors and sealing steam \*  
 \* to the turbine. Condenser vacuum will decrease to 20" \*  
 \* very quickly, causing the TBV to fail shut. Therefore, \*  
 \* close main steam to aux steam HV-20560 and HV-20565 \*  
 \* last and reopen first (as soon as possible). \*  
 \*\*\*\*\*

3. Isolate both OTSGs

3. Isolate both OTSGs.

- .1 Perform this Step (3.1) ONLY IF OTSG level increases to 95% on the operating range, OTHERWISE CONTINUE WITH STEP

3.2.

- 
- .1 Trip both MFW Pumps.  
 .2 Stop AFW Pump P-318.  
 .3 Start/verify start of Motor Driven AFW Pump P-319.  
 .4 Continue with Step 3.2

- .2 Terminate flow to both OTSG's by closing the following valves.

HIRC or HISS

<u>Valve</u>	<u>A OTSG</u>	<u>B OTSG</u>
AFW Control	FV-20527	FV-20528

HIRI

<u>Valve</u>	<u>A OTSG</u>	<u>B OTSG</u>
S/U FW Control	FV-20575	FV-20576
MFW Control	FV-20525	FV-20526
MFW Block	FV-20529	FV-20530

- .3 If feedwater flow continues, trip appropriate feed pumps to terminate flow.  
 .4 Terminate steaming by verifying valves closed.

Turbine B/P	PSV-20563	PSV-20566
	PSV-20561	PSV-20564
ADV	PV-20571A	PV-20562A
	PV-20571B	PV-20562B
	PV-20571C	PV-20562C

H2SFA and H2SFB

<u>Valve</u>	<u>A OTSG</u>	<u>B OTSG</u>
AFW Bypass	SFV-20577	SFV-20578

H2YS

<u>Valve</u>	<u>AOTSG</u>	<u>BOTSG</u>
MS Aux FWP	HV-20569	HV-20596
Main Stm to Reheaters	HV-20598	HV-20597
Pegging Stm	HV-32243	
Main Stm to Aux Stm	HV-20565	HV-20560

The procedural guidance available to the operators in E.02 and E.05 assumes that ICS is available so that operators can control all ICS valves from the control room. This, however, was not the case during the December 26, 1985 incident. Thus, until ICS power was restored, the operators were fully engaged in trying to carry out Step 1 of E.05 from within the control room and Step 3 of E.05 outside the control room by manually operating the valves locally.

Based on Step 1 of E.05, the operators were attempting to re-establish pressurizer level to 100 inches by starting an additional high pressure injection (HPI) pump and increasing HPI injection flow to the RCS. Shortly after operators started these tasks, the safety features actuation system (SFAS) initiated on low RCS pressure and commenced full HPI. Although RCS pressure had gone down significantly as the result of the overcooling, and the pressurizer level indication went off scale low, the RCS subcooling margin was always well in excess of minimum requirements. RCS pressure started to increase prior to the pressurizer level being re-established on the indicating range; and, at this point, the operator started to throttle back on HPI, even though the operators had not restored pressurizer level to above 100 inches, as required by the operating procedures. The operators realized that they had sufficient subcooling margin and that as RCS pressure increased, and RCS temperature remained low, they would enter the pressurized thermal shock (PTS) region.

E.05, Step 1 states, "Maintain pressurizer level above 100 inches," a statement further qualified by "IF pressurizer level cannot be maintained above 100 inches THEN initiate Full HPI (Rule 1 and 2)." However, Rule 2 states "HPI should be throttled to prevent exceeding the reactor vessel pressure temperature limit...during OTSG cooling or HPI cooling." Further, Rule 6 states, "if [RCS temperature dropped below 500°F and exceeded a 100°F/hr cooldown rate]... stabilize temperature and pressure below the [PTS region]. Depressurize."

In discussions with some of the B&W personnel involved in the development of vendor ATOGs, they indicated that there was a conscious effort to de-emphasize the importance of pressurizer level as long as a subcooling margin could be maintained. It does not appear that the plant procedures or operator training reflected this priority.

The Team finds that the EOPs at Rancho Seco do not address the loss of ICS. The lack of specific guidance seems to be a weakness in the plant-specific EOPs available to the operators on December 26, 1985. The Rancho Seco ATOGs supplied by the B&W Owners Group provide for the loss of ICS and non-nuclear instrumentation (NNI) power. The ATOGs direct the operator to an explicit procedure to be followed when a loss of ICS power occurs. However, this procedure was not included in the Rancho Seco EOP. It appears that SMUD did not consider the loss of ICS dc power to be a credible event and therefore did not consider it necessary to include procedural guidance on the loss of ICS dc power in their EOPs.

The Annunciator Procedures Manual provided additional procedural guidance that was intended to be used by the operators in conjunction with annunciator alarms. The procedure for the "ICS or Fan Power Failure" alarm includes four steps. Step 1 requires that operators ensure that the automatic bus transfer (ABT) device has transferred from its normal to its alternate power supply. (This did not happen during the December 26, 1985 incident because the normal power to the ABT was not lost.) Step 2 of the procedure does not involve

operator action, but provides a basic explanation of the 24 Vdc power supply. Step 3 tells the operators how to reset the ABT device in the event normal power is restored. Finally, Step 4 indicates how operators should restore cooling given a fan failure alarm, which is one of the trouble alarms associated with the same annunciator that is used for ICS power failure.

The Annunciator Procedures Manual was not used by the operators following the "ICS or Fan Power Failure" alarm. Even if it had been used, it contained very little guidance concerning the implications of the alarm and would have been of no value to the operators in recognizing or restoring the loss of ICS dc power.

Finally, procedures C.13A and C.13B provide operators with guidance for plant shutdown from outside the control room. These procedures include operating ADVs and TBVs using an alternate system that is independent of ICS power. This alternate system was installed as part of plant modifications for fire protection.

All operators had received extensive training on this recent plant modification and the alternate system for operating the ADVs and TBVs. However, the training emphasized the use of these procedures only after evacuation of the control room following a fire. It appears that SMUD did not consider incorporating these control provisions in procedures governing plant conditions other than a fire in the control room.

The operators did not remember that these alternate methods of operating the TBVs and ADVs existed and there was no guidance in the operating procedures directing them either to the switches controlling the TBVs and ADVs or to other procedures explaining their location. Therefore, this available method to remotely operate the TBVs and ADVs was not used, and local manual operation was pursued by the operators.

#### 6.5 Compliance With Procedures

As noted earlier, Step 3 of Procedure E.05 directed operators to isolate the OTSGs. In the December 1985 incident, with no ICS dc power available, operators were dispatched to the valves to operate them manually to isolate the OTSGs. The procedure goes on to say "if feed flow continues, trip appropriate feed pumps to terminate flow." The operators were able to isolate all sources of steam from the OTSGs by manually closing the valves locally. However, they were not able to isolate feed flow to the OTSGs before power was restored to the ICS (i.e., the A AFW (ICS) flow control valve had failed open, and the manual isolation valve was stuck open). Therefore, they were unable to terminate flow to the OTSG. During the time operators were trying to isolate the OTSGs, the Shift Supervisor and some of the other licensed operators discussed maintaining a source of AFW to the OTSGs. The decision was made at that point not to trip the AFW pumps unless there was danger of overflowing the OTSGs and possibly damaging the turbine-driven AFW pump as a result of water overflowing into the main steamlines.

A few minutes into the event, OTSG level was regained and continued to rapidly increase until it went off-scale high about 18 minutes into the incident. When the OTSG level increases to 95 percent on the operating range, the procedure (E.05, Step 3) directs operators to stop the turbine-driven AFW pump and start

the motor-driven AFW pump. However, this action was not taken and both AFW pumps continued to pump water into the OTSGs. As a result, the OTSG levels continued to increase and water started overflowing into the main steam lines associated with the A OTSG. The operators did not adequately monitor the OTSG levels to determine when to stop the AFW pumps. Thus, the decision not to trip the AFW pumps created a situation that required frequent monitoring of OTSG levels to determine when action was required. When operators failed to monitor the OTSG levels and thus did not recognize that conditions existed that required that they take action, the A OTSG overflowed. The operators' reluctance appears to be the result of the substantial emphasis placed on the AFW system by NRC and others, and a lack of confidence in the reliability of the AFW pumps (i.e., fear that the pumps would not restart if stopped).

Finally, Rule 3, "Feedwater Throttling Guidelines," gives operators explicit guidance to stop AFW flow during overcooling events. Rule 3 states:

### RULE 3 - FEEDWATER THROTTLING GUIDELINES

#### 1. AFW THROTTLING GUIDELINES

- .1 If a cooldown is required, THEN throttle AFW as necessary to Limit the cooldown rate to less than the maximum allowed 100 F/hr.
- .2 Maintain continuous AFW flow until the appropriate level set-point is reached. Do not allow the OTSG level to decrease if level is still below the appropriate level.

Exception - If excessive primary to secondary heat transfer exists THEN stop AFW flow to the steam generator(s) being over cooled.

#### 2. AFW THROTTLING WITH RCPS OFF

- .1 Do not throttle AFW If
  - .1 Natural circulation has stopped
  - .2 AFW actuation was delayed after loss of RCPS
  - .3 AFW is feeding only 1 OTSG
- .2 Throttle AFW when
  - .1 Level reaches 95% on operate range
  - .2 Natural circulation is verified.

Guidance to the operators in executing the EOPs is provided in the form of rules. They accompany the EOPs and are referred to parenthetically in the EOPs where appropriate to the task operators are undertaking in the EOP. The operators are expected to commit the rules to memory because their significance at times transcends the apparent intent of the procedural step, e.g., maintaining pressurizer level vs. subcooling margin; feeding OTSG in an overcooling event.

It is apparent to the Team that the operators neither applied nor understood the significance of the EOP rules applicable to the December 26, 1985 incident.

#### 6.6 Role of the Shift Technical Advisor

When this event began at 4:14 a.m., the Shift Technical Advisor (STA) was asleep in the onsite trailer provided for that purpose. At Rancho Seco, the STA is licensed as a Senior Reactor Operator. He is onsite for a 48-hour period of duty and is required to be in the control room for the beginning and turnover of each shift during that 48-hour period. He had participated in the shift turnover at midnight and retired at approximately 2:00 a.m. The STA was awakened by the noise created by the lifting of the OTSG code safety valves and the ADVs. He dressed quickly and went to the control room, stopping at the turbine deck on his way to see if any of the safety valves that lifted had failed to reseat. Once in the control room, he assessed the situation and then conferred with the Shift Supervisor on the status of the plant. The STA inspected the ICS panels to see if he could determine the reason for the loss of power. He noted that the pilot lights on the ICS dc power supplies were off and that the ABT was selected to its normal source of power. He does not remember looking at switches S1 and S2.

Apparently, when the STA investigated the loss of ICS power, he did not adequately understand the system configuration. As can be seen in Figure 3.5, with power still available on the 1C bus (i.e., the ABT had not transferred) and the ICS dc power supplies de-energized, the most credible cause for the ICS power failure was the opening of switches S1 and S2.

While the STA was in the vicinity of the ICS cabinets, the backup Shift Supervisor recognized that switches S1 and S2 had tripped to the OFF position. He asked the STA if he thought it was all right to close the switches, at which time the STA said "Yeah, go ahead. It can't hurt us."

In an interview with the Team, the STA was questioned about plant conditions, his awareness of the subcooling margin that the plant had attained, and his concern over PTS. He indicated that he was very concerned about PTS. In fact, he said, at one point he did a calculation of the subcooling margin and concluded that, "Even with almost no pressurizer level, we were pretty deeply into thermal shock." However, he did not recommend that the AFW pumps be secured because he was not asked to provide guidance by the operators.

Recognizing that the STA's role is to provide engineering expertise on shift, the Team tried to ascertain to what extent the STA filled that role during this event. Neither the operators nor the STA could identify an instance of when the STA provided expertise during the incident. However, the operators quickly volunteered that the STA was valuable as an extra person on shift to help out during the incident. The Shift Supervisor asked the STA to inform management personnel of the event and to call in extra help. The Team concludes that although the STA on shift was useful as an extra person, he did not provide the type of engineering expertise that may have been useful in identifying the cause of or in mitigating or terminating this incident.

## 6.7 Licensed Operator Training

The Team reviewed licensed operator training for how well it prepared operators to recognize and mitigate the transient. The Team learned that during the incident, at least three people went to the ICS cabinets to investigate the loss of ICS power. What they observed was that the 120 Vac ABT was still on the vital IC bus and energized (the normal condition) and that all four 24 Vdc power supplies were de-energized (an abnormal condition). None of the operators understood or recognized that for the situation they observed, switches S1 and S2 which provide power to the 24 Vdc power supplies, had to be in the OFF position. Some operators reported that they did look at the switches. However, if they did, they failed to recognize that the switches, which are clearly marked, were in the OFF position (see Figure 6.1). In addition, although simplified drawings of the non-nuclear instrumentation (NNI) power supplies were posted on the NNI cabinets, comparable drawings for the ICS power supply had not been provided. Not until about 26 minutes into the event did a more experienced Senior Reactor Operator recognize that S1 and S2 were OFF. After consulting with the STA, he turned the switches back on, thus restoring ICS dc power.

The fact that several licensed operators did not recognize the improper position of switches S1 and S2 suggests that their on-the-job training did not adequately focus on normal and off-normal ICS power configurations for this crucial system.

Although, the operators receive extensive classroom training in systems and hands-on and simulator training prior to receiving NRC licenses, they do not appear to have been trained in enough depth on the ICS to understand the power supply system that caused the December 26, 1985 incident.

Further, 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 they did receive training on mitigating overcooling events with ICS power available.

During this incident, the operators also isolated the suction to the running makeup pump such that it was severely damaged. When SFAS is initiated at Rancho Seco, the suction valve closes from the makeup tank (MUT) which normally supplies water to the makeup pump. However, the suction valve from the borated water storage tank (BWST) opens to provide water to the makeup pump and the A HPI pump. Earlier in the event, the operators had secured the A HPI pump, which left only the makeup pump running and taking a suction from the BWST. The recirculation flow from the makeup and HPI pumps was going to the MUT, which caused a high level in the makeup tank. The operator shut the suction valve from the BWST to the makeup pump and the HPI pump, thinking that this would cause more water to be drawn from the MUT. However, the operator failed to remember that the suction from the MUT was still shut. By shutting the suction from the BWST, he isolated the sources of water to the running makeup pump.

At the simulator where the operators receive their hands-on training, the suction valve from the MUT remains open on initiation of an SFAS. So, in effect, there are two supplies of water available to the makeup pump. Therefore, shutting the suction valve from the BWST during simulator training would not have

simulated destruction of the makeup pump. The difference between actual system response and simulator response was noted by the instructors and discussed during simulator training. They would initiate an event that included an SFAS initiation. Upon recovery from the SFAS, if the operators failed to simulate reopening the suction valve from the MUT to provide water to the makeup pump, the simulator instructor would "destroy" the makeup pump, reinforcing the fact that the makeup pump no longer had a suction supply. Although they may have forgotten during the event, the operators acknowledged during interviews that they were aware of this difference.

#### 6.8 Nonlicensed Operator Training

Nonlicensed operator training consists primarily of the self-study of systems outlined in a System Study Guide used by those qualifying as Equipment Attendants and Power Plant Helpers. Trainees must initial system checkout sheets when they feel they have sufficient knowledge to satisfy an oral checkout of the complete system. A Shift Supervisor's signature is then required for the oral checkout. In addition to the System Study Guides, they study on-the-job (OTJ) Study Guides with checkout sheets that must also be completed for qualification. OJT is to be completed under the supervision of a cognizant operator who signs and dates the sheet, documenting that tasks have been performed successfully. Each task designated on an OJT checkout sheet must be performed. However, a walk-through may be substituted for those tasks that cannot be performed because of plant conditions.

During this event, the nonlicensed operators were required to manipulate valves in the plant they had been trained to operate, one of which was the AFW (ICS) flow control valve to the OTSG. An operator did not accurately determine the position of the valve when using the manual handwheel mechanism to close the valve. Although position indicators are mounted alongside the valve stem, the operator did not use it to determine the valve position. Even if it had been used, the accuracy of the indicator is questionable because of the poor gradation and marking on the scale and the existence of a 1/8-inch separation between indicator discs (see Figure 6.2). In addition, the position indicator is located such that the operator cannot see it directly while operating the handwheel (see Figure 5.2). The valve stem, however, can be observed from the handwheel, and the operator chose to use the amount of visible uncorroded stem, instead of the position indicator gauge, as his indicator of the valve position (see Figure 6.3).

The position indicators provided on the valves were not used by the operators during the December 26, 1985 incident. The operators might have used the sound of water flowing through the pipe as a secondary indication of valve position. That is, the sound of moving water indicates that the valve is not completely closed. However, the lifting of the ADVs and OTSG code safety valves in the general vicinity of the AFW (ICS) flow control valves may have masked the sound of the AFW flow.

A walkie-talkie was given to the nonlicensed operator dispatched to close the AFW (ICS) flow control valves. However, he discovered that transmission from the area where the valves are located to the control room was not possible. The operator had to communicate with the control room using the phone in the evaporator room, approximately 100 feet from the valves. Headsets are available in the area of the valves, but were not used during this event. The



operator did not request AFW flow verification from the control room to determine the valve position.

The operator's manipulation of the handwheel mechanism on the AFW (ICS) flow control valve was not performed in accordance with the valve vendor's instructions. In particular, the air supply and bypass valves on the controller were not manipulated as specified. Although for this event the impact of overlooking those steps was not significant, under other circumstances (e.g., if the valves were reopened to control flow), properly transferring from automatic to manual (local) operation could become more important. At Rancho Seco, manual operation of these valves is relied upon to control AFW flow for certain events.

In summary, an operator applied excessive force to the valve using a valve wrench (cheater) to close the AFW (ICS) flow control valve. He did so because of his failure to determine the actual position of the valve and his desire to ensure that flow was completely shut off. The end result, however, was that the valve reopened and manual capability to operate the valve was lost.

These observations suggest training weaknesses in acceptable use of valve wrenches, the proper methods to manually operate and override air-operated controlled valves, and the use of available and backup indications to determine valve position. These weaknesses suggest areas where hands-on training rather than walk-through or talk-through training may be necessary.

Engineering reports generated during the troubleshooting performed by SMUD indicate that the handwheel mechanism on both AFW (ICS) flow control valves were damaged prior to this incident. It is possible that the existing damage could have made the valve more difficult to operate, thereby contributing to the use of excessive force by the operator.

During this event, the nonlicensed operators were directed to enter the makeup pump room to isolate the makeup pump that had failed earlier. It was suspected, prior to their entry, that there were radiological problems as a result of failure of the makeup pump. Although the operators put on protective clothing, they did not sample the room for airborne radioactivity and did not wear respirators or self-contained breathing apparatus. In addition, they did not wear hightop boots, even though radioactive water was on the floor of the makeup pump room to a depth of approximately 4 inches.

These oversights were caused by a combination of reasons. The proper protective equipment and respirators were not available in the immediate area of the makeup pump room, and operators perceived a sense of urgency on the part of the control room operator who gave them their instructions. The Control Room Operator had expressed a concern that the plant could experience a small loss of coolant accident (LOCA) through the damaged makeup pump. The absence of hightop boots resulted in radioactive contamination of the operators' personal clothing (shoes, socks, trousers). Whole body counts of the operators were subsequently taken and it was determined that internal exposure was negligible.

## 6.9 Radiation Protection and Emergency Plan

The Team decided not to review the implementation of the Rancho Seco radiation protection procedures or emergency plan because NRC Region V conducted a

special inspection to evaluate the licensee's implementation during the December 26, 1985 incident. The results of this inspection are characterized below.

The December 26, 1985 incident resulted in a release of gaseous radioactive material to the auxiliary building which was discharged via the auxiliary building stack to the environment. This release of about 80 curies of radioactive gas did not result in a significant threat to the public health and safety or to individuals working at the facility.

The operators appear to have focused most of their energies on mitigating the plant transient and did not concentrate much attention on implementation of their emergency plan responsibilities. The Shift Supervisor, who also functioned as the Emergency Coordinator, concerned himself with directing actions to bring the overcooling transient under control but did not assure execution of several elements of the emergency plan implementing procedures. Specifically:

- o The event was properly classified in a timely manner; however, the required plant announcement of the declaration of an unusual event was not made. Failure to announce the event over the site public address system resulted in some shift personnel (e.g., chemistry, radiation protection) not being aware of the ongoing problem.
- o The initial notification to state and local agencies was timely but failed to contain all the information required by procedures.
- o Followup information was not provided as stated it would be during the initial notification and as required by procedure, and changes in plant status were not reported (e.g., a radioactive gaseous effluent release rate in excess of the alarm setpoint was not reported to the local offsite authorities).
- o Documentation required by the emergency plan implementing procedures was incomplete.

The Region V inspection also found deficiencies in the content of several emergency plan implementing procedures related to radioactivity release alarm setpoints, assessment of offsite dose, and documentation requirements. These deficiencies were not a major factor during the December 26, 1985 incident. Emergency plan implementing procedure training had been held as required, but was generally noted as being deficient by the operators.

Historically the licensee has considered the operators to be qualified in radiation protection and has permitted them to take action independent of the radiation protection organization. This philosophy prevailed during the December 26, 1985 incident and resulted in two nonlicensed operators entering the makeup pump room to isolate the makeup pump without first informing the onsite radiation protection technician.

The effluent release resulting from the makeup pump failure caused the auxiliary building vent monitor to alarm. The Region V inspection followup revealed:

- o The control room operators were faced with three conflicting alarm setpoints for the same parameter. The procedure in the Annunciator Procedure Manual for the auxiliary building vent monitor contained a statement about the monitor setpoint that was not correct. The actual alarm setpoint for the vent monitor was correct but was different from the alarm setpoint of the auxiliary building accident radiation monitor required by NUREG-0737. There was no procedure for operator response to the accident radiation monitor.
- o The Emergency Coordinator directed the radiation protection technician to perform a Maximum Permissible Concentration (MPC) determination at the site boundary. The technician could not locate the procedure and failed to collect the required stack sample; however, he did perform a reasonable evaluation based on the accident radiation monitor reading and on his professional experience.
- o The onshift crew did not make an offsite dose projection. The radiation protection technician had not been trained in the procedure and the procedure provides no method to project offsite dose resulting from sources originating from a primary to secondary leakage pathway.
- o The auxiliary building vent monitor multipoint recorders failed to provide a trace for review. One recorder was not inking, the other produced an illegible trace.
- o An evaluation made by the Radiation Protection Manager later on December 26, 1985, using data from the accident radiation monitor and a stack sample taken at 0825 PST, found no detectable iodine or particulate activity and projected the whole body dose at the site boundary resulting from the noble gas release to be 0.2 millirem. This value was calculated using conservative accident methodology; a re-evaluation using more precise techniques will result in a dose estimate less than this value.

While the above deficiencies in SMUD's radiological control and emergency preparedness programs during the December 26, 1985 incident did not jeopardize the public health and safety due to the relatively minor radiological consequences of this incident, they do indicate weaknesses in SMUD's program and training of Rancho Seco staff.

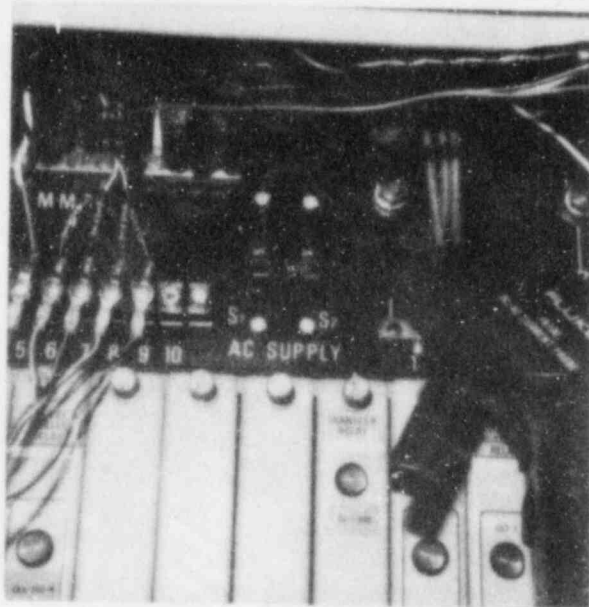
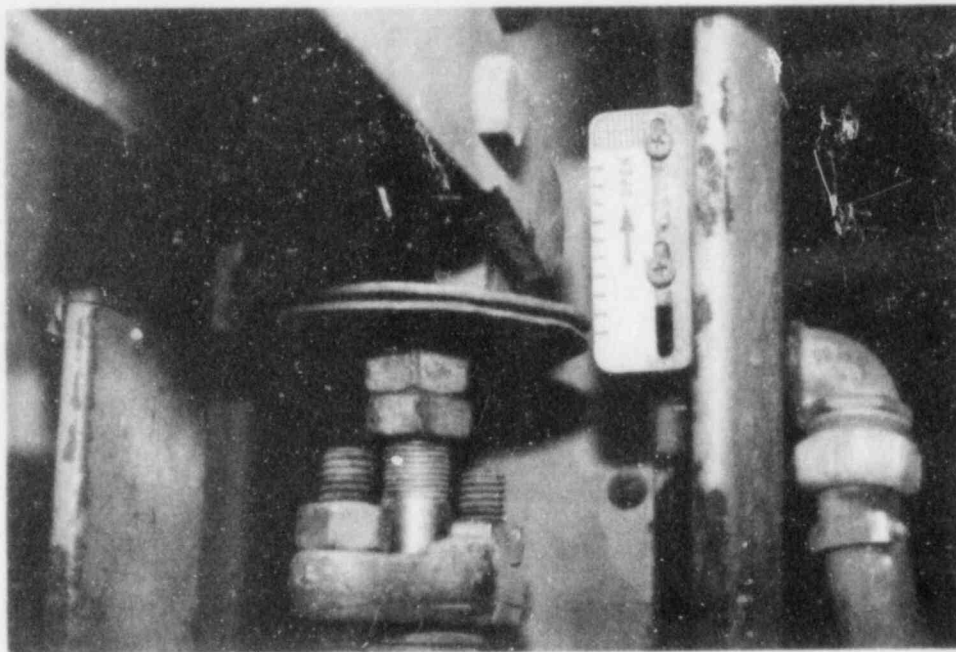


Figure 6.1 Switches S1 and S2 in the tripped (OFF) position



(PHOTO RETOUCED)

Figure 6.2 Position indication on AFW (ICS) flow control valve

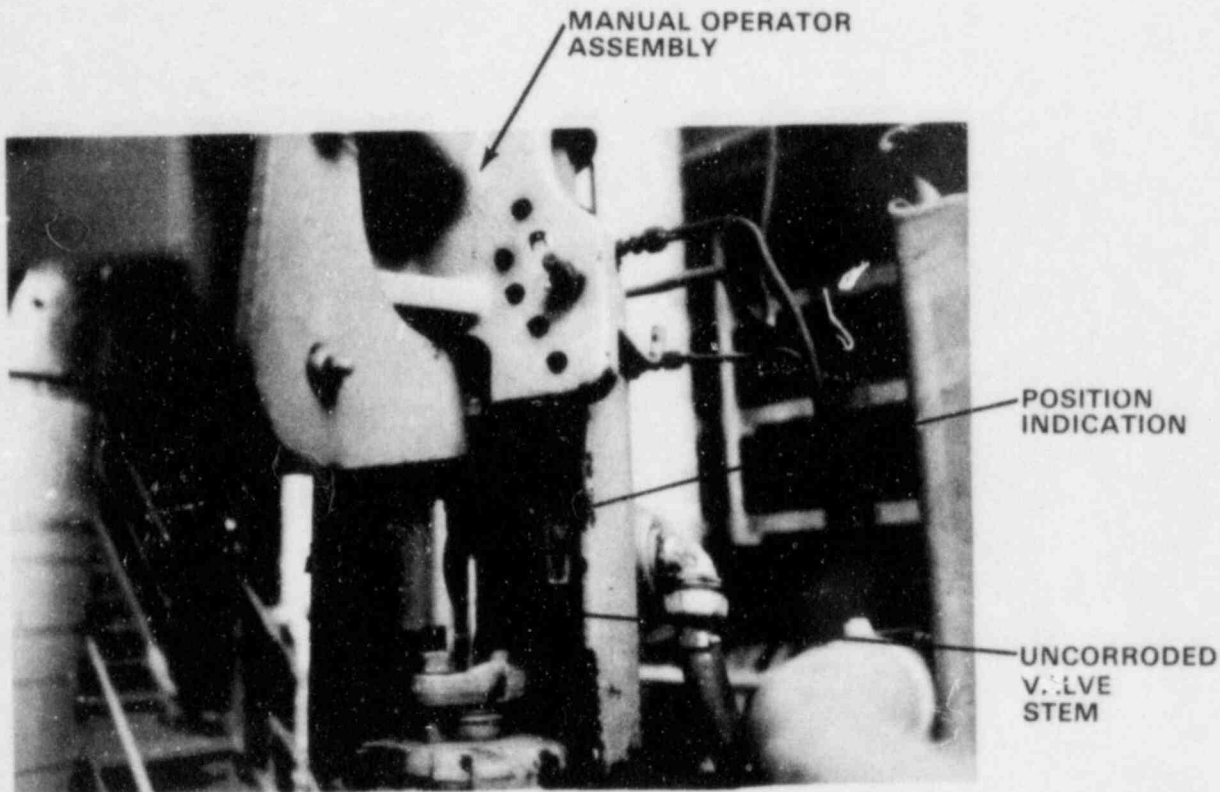


Figure 6.3 A AFW (ICS) flow control valve (FV-20527)

## 7 PRECURSORS TO THE DECEMBER 26, 1985 INCIDENT AT RANCHO SECO AND RELATED NRC AND SMUD ACTIONS

### 7.1 Response of B&W-Designed Plants to Failures of the ICS and NNI

One significant aspect of the December 26, 1985 event was that the loss of the nonsafety-related integrated control system (ICS) resulted in the plant being subjected to a significant overcooling transient. In the course of mitigating this transient, operators were required to take a number of actions for which only limited procedural guidance was available. Since the response of Babcock & Wilcox (B&W)-designed plants to transients initiated by loss of non-nuclear instrumentation (NNI) and/or ICS has been raised on numerous occasions in the past (see Table 7.1 and Figure 7.1), the Team reviewed the principal precursor events and subsequent Sacramento Municipal Utility District (SMUD) and NRC actions in the context of how they apply to the December 26, 1985 incident.

Section 7.1.1 discusses the March 20, 1978 loss of NNI power at Rancho Seco, which was subsequently reviewed by SMUD and NRC. Section 7.1.4 discusses the loss of NNI/ICS that occurred at the B&W-designed Oconee plant on November 10, 1979, including SMUD's and the NRC's review of IE Bulletin 79-27 which was issued as a result of the Oconee event. Section 7.1.4.1 describes the loss of NNI power that occurred at the B&W-designed Crystal River plant on February 26, 1980. Section 7.1.5 describes NUREG-0667, which considers the response of B&W-designed reactors to various transients, including a loss of ICS power. Section 7.1.6 discusses the NRC review of a partial loss of NNI power that occurred at Rancho Seco on March 19, 1984. Finally, Section 7.1.7 describes the NRC review done under Unresolved Safety Issue (USI) A-47.

Rancho Seco received its operating license on August 16, 1974. When the NRC staff reviewed SMUD's applications for a construction permit and an operating license, the ICS was considered a nonsafety-related control system and so was not reviewed in detail. The principal focus of the licensing review was to ensure that a failure in the ICS would not interfere with the performance of protection systems (i.e., reactor trip system, and safety features actuation system).

During its first year of operation, Rancho Seco underwent several transients caused by loss of power to the ICS. These transients occurred because the ICS had only a single 120 Vac power supply (i.e., the system lacked a backup power supply). As a result of these transients, SMUD modified the ICS in 1975 to provide a redundant power supply.

#### 7.1.1 The Rancho Seco Lightbulb Incident

On March 20, 1978, Rancho Seco underwent a severe transient as a result of a loss of power to NNI, which provides the input signals to the ICS. During this event, which has come to be known as "the lightbulb incident," an operator was removing a light bulb from a back-lighted push button in the control room. While handling the bulb, he dropped it into the cavity left after removing the bulb retainer. This caused a short circuit on the -24 Vdc NNI-Y power system,

which was not adequately fuse-protected. The power supply monitor for the NNI-Y detected the low bus voltage caused by the short circuit and tripped the 120 Vac input switches (S1 and S2). Although the initial problem occurred in the NNI system, it resulted in a mid-scale failure of signals being sent from the NNI to the ICS. The loss of a large percentage of NNI instruments initiated a plant transient and caused the failure of control room instrumentation usually used by operators to determine plant conditions. Although the cooldown rate of the primary system was excessive (the plant cooled down 300°F in 80 minutes), the operators were able to stabilize the plant. During the event, the safety features actuation system (SFAS) actuated automatically because of low RCS pressure.

Following this event, SMUD was concerned that this procedurally unrehearsed situation had caused considerable uncertainty with respect to the validity of the instrumentation in the control room. As a result, SMUD conducted an extensive review of the event. The specific changes made as a result of this review include:

- o installation of changes in the light socket design to reduce the likelihood that a dropped lightbulb would cause a short circuit
- o installation of lower-rated fuses to provide faster clearing of faults
- o installation of a separate power supply system for NNI instrument selector switches
- o installation of fuses in NNI circuits that previously had no fuses
- o installation of new instrumentation that was independent of NNI
- o preparation of procedures for loss of NNI and training of the operators on the use of the procedures

Although the ICS power supply is similar to the NNI power supply, particularly with respect to the role of the power supply monitor, SMUD's principal emphasis was on the NNI rather than on both NNI and ICS. For example, similar changes were not made to the ICS power supply, and no procedures were developed or training conducted for the loss of ICS power. The emphasis on NNI seems to have biased SMUD's subsequent reviews of issues associated with the NNI and ICS.

#### 7.1.2 The First Rancho Seco Loss of ICS Incident

One year later, on January 5, 1979, a reactor trip occurred which included the loss of ICS power at Rancho Seco. The trip was caused by a short-to-ground in the ICS and resulted in a subsequent reactor cooldown which again exceeded the limits in the plant Technical Specifications. (The reactor coolant system was cooled by approximately 120°F in 15 minutes.) During this event, a technician performing a modification to the ICS accidentally shorted the circuit to ground, causing the 24 Vdc power supply monitor to trip. The loss of power resulted in the feedwater valves going to the mid-stroke position, which caused the reactor coolant system pressure to increase, causing a reactor trip. Subsequent overcooling caused RCS pressure to decrease, causing SFAS actuation, which in turn caused AFW to initiate. Thus, the course and consequences of this event were



very similar to the December 26, 1985 incident. During the 1979 event there was a compounding problem of a switch error that caused a lack of indication of SFAS Channel A actuation, a condition which tended to further confuse the operators.

This event was reported to NRC in a Licensee Event Report (79-01) and was reviewed by the NRC as part of its routine inspection program.

The January 1979 incident was not as severe as the lightbulb incident and did not receive the same level of attention. SMUD made no changes in the design of the ICS and procedures for loss of ICS power were not developed.

### 7.1.3 BAW-1564 "Integrated Control System Reliability Analysis"

The accident at Three Mile Island on March 28, 1979, focused attention on B&W-designed plants and on their response during transients. One outcome of the accident at TMI was that NRC compiled an extensive list of TMI actions items. One of these (II.K.2.9) was a requirement to prepare a reliability analysis of the ICS. This analysis was performed generically by B&W and the results of that analysis are documented in B&W report BAW-1564, "Integrated Control System Reliability Analysis," which was completed in August 1979.

The report included a generic failure modes and effects analysis (FMEA) of the ICS (which happened to be based on Rancho Seco). A number of issues from the B&W report are relevant to the December 26, 1985 incident.

- o The B&W report noted that the most prevalent malfunctions and failures associated with the ICS were the power supplies associated with the ICS. Specifically, the ICS and NNI power supplies are vulnerable to single failures with significant consequences. (A single failure in the ICS power system initiated the December 26, 1985 transient.)
- o When the report was prepared, approximately one-third (101 of 310) of the reactor trips at B&W-designed plants were caused by problems associated with the ICS.

The report includes a number of recommendations concerning areas for enhanced reliability and safety. Among the recommendations relevant to the December 26, 1985 incident were concerns about NNI and ICS power supply reliability. The report notes that these power supplies have a relatively significant failure rate and should be improved to enhance plant availability. By letter dated November 7, 1979, NRC requested that SMUD provide its position on the recommendations contained in BAW-1564. Some additional expansion of the recommendations was included in the NRC request.

BAW-1564 was also reviewed by the Oak Ridge National Laboratory (ORNL) under contract to NRC to determine the adequacy of the B&W analysis.

The ORNL analysis, submitted to NRC on January 21, 1980, noted that B&W-designed reactors appear to be unusually sensitive to certain off normal transients originating in the secondary system, and one of the features that contributes to this sensitivity is the B&W reliance on an ICS to automatically regulate feed-

water flow. In addition, the ORNL analysis concluded that the B&W analysis was more notable for what it did not include than for what it did include.

Specifically, the ORNL report noted that although the ICS controls the operation of equipment that is important during post-trip situations, the B&W analysis did not include this aspect. For example, the report noted that the ICS could cause a loss of main feedwater and also could inhibit auxiliary feedwater via the flow control valves. This possibility was not addressed by B&W presumably because it was a plant-specific issue. The ORNL report concluded that the scope of the B&W analysis was very limited. The ORNL analysis took into account this limited scope and attempted to evaluate the analysis presented and to suggest additional work which might be done to achieve the original objectives.

ORNL found no evidence that the ICS provided more frequent or more severe challenges to the plant protection system (PPS) than other control systems of similar scope or that these challenges exceeded the PPS capability. It went on to agree that the ICS should not be classed as a protection system, but that there should be more concern for avoiding degradation of failures within the system. ORNL made recommendations they believed would meet the original study objective desired by NRC. One of these recommendations states:

Power supply failures have caused and are continuing to cause significant plant upsets. They should be evaluated in detail and specific recommendations for their upgrading should be required.

On the same day that the ORNL review was submitted to NRC, SMUD submitted a letter providing their position on the recommendations in the B&W report. NRC requested that SMUD discuss the need for additional training of operators concerning design and/or operational problems in the feedwater and related systems. SMUD's response, however, noted that they had three operating procedures that provided the majority of the ICS operating guidance: the System Operating Procedure (A.72), the Plant Heatup and Startup Procedure (B.2), and the Plant Shutdown and Cooldown Procedure (B.4). They also noted that ICS training typically consisted of several days of formal classroom lectures and audio-visual training. They provided an outline of the course content. Although the outline included an extensive discussion of the operation of the ICS, it did not include any indication that failure of the ICS and the subsequent plant response was included in the training. The outline noted, however, that B&W simulator training provided extensive and worthwhile operational experience on the ICS.

In general the response points out that some modifications were being considered, although it does not appear that SMUD committed to making any substantive changes as a result of the recommendations contained in the B&W report.

The NRC Office of Nuclear Reactor Regulation (NRR) subsequently reviewed this material submitted in late 1979 and early 1980 by B&W, ORNL, and SMUD. On January 13, 1982, NRR responded that they considered item II.K.2.9 of the TMI Action Plan (NUREG-0737) to be closed for Rancho Seco. They further noted that control systems that affect plant safety would be reviewed under Unresolved Safety Issue (USI) A-47. They found that the Rancho Seco design met all current regulatory requirements and that they had not identified any control system failures or actions that would lead to unacceptable consequences at Rancho Seco.

In summary, in March 1979, B&W issued a report (BAW-1564) in which they analyzed the reliability of the ICS. Although the B&W analysis noted a number of changes that appeared to be warranted in the ICS, SMUD concluded that no changes were necessary. A subsequent analysis of the ICS by the Oak Ridge National Laboratory criticized the B&W analysis and noted that it was of limited scope and did not appear to meet the requirements of the original Order. The NRC staff concluded that no immediate changes were required at Rancho Seco as a result of the B&W analysis. The long-term issues associated with the B&W report were to be considered in Unresolved Safety Issue (USI) A-47, "Safety Implications of Control Systems."

#### 7.1.4 IE Bulletin 79-27, "Loss of Non-Class-1E-Instrumentation and Control Power System Bus During Operation"

During the period that the NRC staff and SMUD were reviewing the analysis performed by B&W, an event occurred at the B&W-designed Oconee plant on November 10, 1979. During the event, a non-Class 1E inverter that fed all power to the ICS and to one channel of NNI tripped due to a blown fuse. The ABT failed to automatically transfer the loads from the inverter to the alternate regulated ac power source. All valves controlled by the ICS assumed their respective failure positions and the operators lost most indication in the control room. The loss of power lasted for approximately 3 minutes. The NRC sent a senior technical reviewer to Oconee who noted that this event and the lightbulb incident at Rancho Seco had resulted in the loss of practically all control room indication that the operators normally used. The reviewer was also concerned about the loss of plant control that could result from such a loss of power. As a result, the reviewer concluded that NRC should issue a Bulletin so that the NRC could become more involved with non-class 1E systems.

As a result, Bulletin 79-27, issued on November 30, 1979, was sent to all operating reactors, including Rancho Seco. The Bulletin required a number of actions:

1. Review the class 1-E and non-class 1-E buses supplying power to safety and nonsafety-related instrumentation and control systems which could affect the ability to achieve a cold shutdown condition using existing procedures or procedures developed under below:
  - o 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.
  - o 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.
  - o 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 nonsafety-related instrument and control systems...

3. Re-review IE Circular No. 79-01, 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. Based on a review of operating experience and your re-review of IE Circular No. 79-01, describe any proposed design modifications or administrative controls to be implemented as a result of the re-review.
4. Within 90 days of the date of this Bulletin, complete the review and evaluation required by this Bulletin and provide a written response describing your reviews and actions taken in response to each item.

The original response from SMUD was submitted by a letter to NRC Region V dated February 22, 1980. In response to the requirement to, "identify the instrument and control system loads connected to the bus and evaluate the effect of loss of power to these loads," SMUD identified and described approximately 20 separate loads. For the ICS they concluded:

The effect of a loss of power to ICS will result in a power transfer of the ICS via an automatic transfer to a non-Class 1E bus. Therefore, a loss on this channel will not have an 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 mode is that all control devices will revert to their 50% position.

The Bulletin required licensees to "[E]valuate the effect of loss of power to these loads." The SMUD response did not appear to be consistent with the original requirement in the Bulletin because it assumed that the power would merely transfer to an alternate power source. During the Oconee event there were two power sources available and the loss of power to the ICS and the NNI was caused by a failure of the power transfer device (ABT) to transfer from one source to the other. Thus, SMUD's response appeared to state that the Rancho Seco design was similar to Oconee and, therefore, was susceptible to exactly the concern raised by the Oconee event. In spite of this, SMUD concluded that a loss of power would have no effect on operation of the ICS. Finally, SMUD did not propose any plant modifications as a result of this analysis.

In response to Item 2, which directed that SMUD prepare emergency procedures or review existing procedures for loss of power to each Class 1E and Non-Class 1E bus, the SMUD response noted:

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

Again, this response did not appear to be consistent with the original concern raised by the Oconee event.

It appears from Team interviews with personnel at SMUD that their focus at that time was on the NNI, particularly because of the light bulb incident which was

by far the most significant off-normal event in the history of the plant. The only real concern about the ICS was loss of NNI signals to the ICS. SMUD felt that they had made major design changes (see Section 7.1.1 ) during the late 1970s and early 1980s as a result of the lightbulb incident. However, in their initial response to Bulletin 79-27, they did not discuss the modifications that they had made as a result of the lightbulb incident. In addition, there appears to be some difference in interpretation between SMUD and the NRC about what constituted a "bus" and what constituted a "load."

Finally, there seems to have been considerable confusion at SMUD over the scope of a procedure covering the loss of ICS, and thus the need for the procedure. The confusion centered on whether the procedure would address how to restore power to the ICS, or whether it would address how to most efficiently operate the plant assuming ICS was lost and could not be immediately restored. In any case, no procedure addressing either option was prepared.

In summary, although the Oconee event, as described in Bulletin 79-27, raised significant concerns about the consequences of a loss of power to B&W instrumentation and control systems, SMUD concluded that no additional design modifications were necessary, and that event-oriented procedures to deal directly with such events were not necessary.

#### 7.1.4.1 Crystal River Event on February 26, 1980

On February 26, 1980, an event occurred at the B&W-designed Crystal River plant which is relevant to Bulletin 79-27. During this event the power supply monitor tripped the NNI power supplies. In this case, however, the loss of power was caused by a "load-side" problem which caused the power supply monitor to de-energize the power supplies, rather than a "supply-side" fault, as had occurred at Oconee. Either problem has the same basic result: a loss of NNI and/or ICS power.

As a consequence of this event, NRC issued an Information Notice (80-10) to all licensees. The Information Notice stated, "IE Bulletin 79-27 was intended to cause licensees to investigate loss of individual power supplies as well as total loss of an inverter or vital bus. An addendum to IE Bulletin 79-27 is planned to be issued in the near future to reflect the CR-3 event." NRC also convened a meeting on March 4, 1980, that SMUD attended. Subsequently, NRC sent a letter to SMUD and other licensees for B&W-designed plants on March 6, 1980 requiring that certain information, in addition to that required in Bulletin 79-27, be provided to enable NRC to determine whether each license should be modified, suspended, or revoked. Among the information required was:

- o A summary of NNI and ICS power upset events that had previously occurred at each plant,
- o The feasibility of performing a test to verify the reliable information that remains following various NNI and ICS power upsets, and
- o An expansion of the review under IE Bulletin 79-27 to include the implication of the Crystal River event.

In their response of March 12, 1980, SMUD summarized the power upset events on NNI and ICS, including the January 5, 1979 event at Rancho Seco (see Section 7.1.2). The discussion noted that "During maintenance, a short to ground

caused ICS power supplies to trip. Automatic control was lost. Excessive cool-down resulted from subsequent SFAS initiation of auxiliary feedwater." The response also contained a lengthy description of a SMUD presentation at the March 4, 1980 meeting, which described in detail the previous Rancho Seco "lightbulb incident" and subsequent plant modifications.

In March 1980, the NRC issued Orders to the licensees of B&W-designed plants requiring three major actions to improve plant system responses to the loss of NNI power.

Subsequent to the event at Crystal River, the newly formed NRC Office for Analysis and Evaluation of Operational Data (AEOD) sent a reviewer to Crystal River to look for issues not already identified by the review teams sent from IE and NRR. One issue which is relevant to the December 26, 1985 incident was documented in a memo dated May 23, 1980 from AEOD to NRR. It noted that one issue identified by the licensee as requiring correction prior to restart of Crystal River was, "Provide override closure of atmospheric dump valves upon loss of ICS power," because the ADVs at Crystal River opened halfway upon ICS power failure. AEOD concluded that it was not clear which other B&W-designed plants had the same design deficiency and whether or not they had reliable ADV position indication available to the operators. The memo recommended that the ADV design deficiency should be corrected expeditiously. AEOD requested that NRR determine whether this deficiency was present at other plants and if so ensure that it was corrected on a timely basis.

Accordingly, by letter dated August 15, 1980, NRR requested information from SMUD concerning the operation of the ADVs following failure of the NNI or ICS power supplies. SMUD responded that: (a) upon loss of ICS power, the ADVs go to the 50 percent open position and valve position indication is lost, and (b) on loss of NNI power, the failure mode of the valve depends on the specific mode of power failure. The SMUD response did not include the information that the TBVs and other valves associated with the AFW and MFW also go to the 50 percent open position on loss of ICS power. Whether this fact was merely overlooked or was recognized but not described is not clear from the information available.

By internal memo dated July 21, 1980, the NRC staff noted that they were forwarding their position on the design deficiency at Rancho Seco to SMUD requesting correction in the near future or justification for continued operation. The memo further noted that correction of this specific design feature did not preclude other single failures from causing overcooling transients. Actions to reduce the likelihood of such transients would be included in the implementation of NUREG-0667. The memo concluded that the staff was currently in the process of allocating priorities for the resolution of the full range of B&W design problems, and that the ADV problem was to be included.

From subsequent correspondence between the NRC and SMUD, it would appear that the correction of the ADV control and override design deficiency was to be included in the emergency feedwater initiation and control (EFIC) system. (See Section 7.2 for a discussion of the regulatory history of EFIC.) The EFIC system is not scheduled for installation at Rancho Seco until 1988.

In summary, from the Team's discussions with SMUD personnel, it would appear that SMUD did not feel that the Crystal River event raised new issues with

respect to Rancho Seco because they had investigated the problem of loss of the +/- 24 Vdc power supplies in the NNI as a result of the lightbulb incident. In addition, they felt that the supplemental material required by NRC regarding the Crystal River event addressed only NNI, not the ICS.

Following the February 1980 loss of NNI power at Crystal River, the NRC identified an issue about the failure mode of atmospheric dump valves (ADV) on loss of ICS power. SMUD's response to this issue did not include the other valves (e.g., TBVs and AFW (ICS) flow control valves) at Rancho Seco that repositioned on loss of ICS power (i.e., they confined it to the narrow issue associated with the ADVs). In addition, SMUD deferred this narrow issue to installation of the EFIC system, which to date has not been installed at Rancho Seco. The NRC found this response to be acceptable.

#### 7.1.4.2 NRC Review of the Responses to Bulletin 79-27

The review of the information provided by SMUD in response to Items 1 and 3 of Bulletin 79-27 was assigned to NRR. Responsibility for the review of Item 2 remained in IE.

The degree to which Item 2 (preparation of emergency procedures to deal with a loss of instrumentation or control system power) was reviewed by IE was difficult to determine. However, it appears from the documentation available that the review consisted of inspections at Rancho Seco during May 1980 which indicated that implementation of the commitments was verified by the NRC Resident Inspector. The reports note that casualty procedures were prepared for loss of NNI and that licensed operators were trained on the use of these procedures. There was no statement concerning the adequacy of the procedures or the training. This is the only information available to the Team concerning the review and close-out of Item 2 of Bulletin 79-27.

With respect to Items 1 and 3, a technical review branch of NRR originally intended to perform an in-depth review comparable to the review that would be conducted as part of the operating license review of a new facility. However, by September 1980, it was concluded that very few of the licensees' submittals contained sufficient information to permit the in-depth review anticipated. As a result, a lengthy supplement to Bulletin 79-27 was prepared and proposed for issuance.

The supplement to Bulletin 79-27 was reviewed by IE which determined that this supplement required more information than should be expected in response to a Bulletin. IE was also concerned that the proposed supplement was being submitted in advance of completing the review of the information that was already available. Thus, IE decided not to issue the proposed supplement to the Bulletin. Subsequently, it was agreed to prepare a supplement to the Bulletin that would be narrower in scope, requiring only that licensees take certain actions to ensure the adequacy of plant procedures for accomplishing cold shutdown. The second draft Bulletin supplement was prepared by an NRR technical review branch in January 1981. Although the ultimate requirement was for a test, the draft Bulletin would have required a considerable amount of analysis by licensees before the test could be conducted. However, concerns were raised within NRR that the confirmatory test constituted certain risks to the plants which were unacceptable. Thus this supplement to the Bulletin was not forwarded to IE for consideration.

In the summer of 1981, an NRR technical review branch completed its review of the information previously submitted by SMUD and the other licensees. Specifically, for Rancho Seco, they concluded that there was "doubtful assurance" that Rancho Seco was in compliance with the Bulletin. Part of the concern arose from SMUD's assertion that they were in full conformance with the Bulletin without having performed any plant modifications. The staff reviewers were aware of a number of modifications that had been made at Rancho Seco and were concerned because these modifications were not acknowledged in the response submitted.

At this point, the scope of the review had narrowed from an indepth review of SMUD's response to a determination only that there was "reasonable assurance" that SMUD had adequately addressed the concerns in the Bulletin. The broader implication of the issue would be included in USI A-47.

The results of this review were documented in an internal NRR memo dated June 26, 1981. The memo requested that for Rancho Seco and 50 other operating reactors out of the 68 responses for which "reasonable assurance" could not be determined, a draft Bulletin supplement be issued (the third draft supplement to be considered) in order to "elicit just the minimum information necessary to provide reasonable assurance that the basic concerns of the original Bulletin had been satisfied."

For Rancho Seco, the memo concluded that there was "no reasonable assurance" that SMUD satisfied the major concerns of the Bulletin, and that SMUD did not specifically state full conformance with all the concerns raised in Items 1 and 3 of the Bulletin.

Specific notes were provided relevant to each plant. For Rancho Seco, the memo notes that a February 22, 1980 response from SMUD states full compliance with Items 1 and 3 without plant modification. A June 20, 1980 letter from Region V to Headquarters identifies numerous related plant modifications, some resulting from the 1978 "lightbulb" incident and others from the CR-3 event.

Despite the request in the June 26, 1981 memo to issue a supplemental Bulletin, it was not issued.

In addition, although the safety issues of the Crystal River event and Bulletin 79-27 appear to have been closely related, the subsequent review of the two events was not closely coordinated. The responses submitted in response to the Crystal River event were not initially forwarded to the NRR technical review branch performing an analysis of the responses to Bulletin 79-27 because they were reviewed directly by a different NRR branch. Based on Team interviews, it appears that there was a sense of urgency associated with the review of the response to the information concerning the Crystal River event, so that review was handled separately from the review of the material submitted in response to Bulletin 79-27.

After the memo in June 1981, the review of SMUD's responses to Bulletin 79-27 was further narrowed to the point where information submitted by SMUD was reviewed only to ensure that there were definitive statements or implications that they had performed the tasks required by the Bulletin. This review included some additional contacts with SMUD. In addition, it appears that by this



point the information from Rancho Seco associated with the Crystal River event was available to the Bulletin 79-27 technical reviewer. The review was documented in an internal NRR memo dated June 1, 1982. This memo concluded that 67 of the 68 operating reactors, including Rancho Seco, had performed the required actions in a manner that satisfied the basic concerns of the Bulletin.

The review concluded that no additional regulatory action was warranted in this area pending delineation of any long-term actions in the context of USI A-47. For Rancho Seco specifically, it was concluded that the required information had in fact been submitted and this item was found acceptable and closed.

In summary, it appears that Bulletin 79-27 was initially intended to solicit detailed information from licensees that could form the basis for an in-depth review of the issues associated with control systems, comparable to the review of safety-related systems as part of an operating license review. Based on the initial scope, the conclusion was reached that SMUD's response did not contain sufficient information and did not adequately address the concerns in Bulletin 79-27. After the progressive narrowing of the scope, it was decided that the responses were adequate, despite what appears to be a number of specific weaknesses in the SMUD response (e.g., the lack of a procedure for loss of ICS). Thus the conclusion was finally reached that SMUD had provided reasonable assurance that they had addressed the concerns in Bulletin 79-27, and that the long-term implications of Bulletin 79-27 would be addressed as part of USI A-47.

#### 7.1.5 NUREG-0667, "Transient Response of Babcock & Wilcox-Designed Reactors"

In late 1979, a special task force was established within the NRC to investigate the apparent high frequency of transients at B&W-designed plants. The task force also assessed the apparent sensitivity of B&W-designed plants to such transients, including the consequences of malfunctions and failures of the ICS and NNI. The product of this study was NUREG-0667, "Transient Response of Babcock & Wilcox-Design Reactors," which was published in May 1980.

Some of the findings contained in NUREG-0667 that are relevant to the December 26, 1985 incident are described below.

- o Operators may be required to take more rapid action and have a better understanding of instrument response than operators in plants having other designs.
- o Regardless of the quality or reliability of ICS and NNI power supply design, power supplies do fail and this may require special procedures and unfamiliar operating modes.
- o The common cause failure potential resulting from ICS failures and interactions has not been adequately determined; the specific example is the Crystal River event.
- o It is a virtual certainty that the operators will face ICS and NNI failures in the future. Improved training of the operators to prepare them for such transients would be of high value.

The report included 22 recommendations, some of which are relevant to the December 26, 1985 incident. Examples of the relevant recommendations are described below. Team comments on the relevance of these recommendations to the December 26, 1985 incident are provided in brackets.

- #5 B&W-designed plants should improve the reliability of the plant control systems particularly with regard to undesirable failure modes of power sources and the ICS itself.
- #5(d) The control systems should have provisions for detecting gross failures and taking appropriate defensive action automatically, such as reverting to manual (i.e., remote) control or some other safe state. [During the December 26, 1985 incident, the automatic and remote control were powered by the same power supply. Thus, loss of power caused loss of both automatic and remote control.]
- #5(f) The recommendations contained in BAW-1564 should receive prompt follow-up action. [The recommendations in BAW-1564 are discussed in Section 7.1.3.]
- #5(h) Prompt follow-up action should be taken on IE Bulletin 79-27. [The follow-up action taken on Bulletin 79-27 is discussed in Section 7.1.4.2.]
- #14 The licensees should develop and implement promptly plant specific procedures concerning the loss of NNI and ICS power. These procedures should be audited by IE. [A loss of NNI procedure exists at Rancho Seco. However, there is no procedure at Rancho Seco for a loss of ICS power.]

The NUREG-0667 recommendations were subsequently prioritized within NRR and the results documented in a memo dated August 8, 1980. The memo noted "In the case of the problem of control system/reactor interactions, we have clearly perceived the problem, as Bulletin 79-27 and NUREG-0667 demonstrates. We have received the industry responses to the Bulletin. We should now proceed with review and take prompt and effective action to insure that incidents such as those which occurred at Rancho Seco, Crystal River Unit 3 and Brunswick Unit 1 will not be repeated."

Of the recommendations from NUREG-0667 that are directly relevant to the Rancho Seco event, the evaluation which forms the basis for the prioritization provides additional insights.

For recommendation 5, which included eight specific recommendations for improvement of the B&W ICS, the prioritization further stated that even though the ICS system was (and is) classified as a control system, its significant impact on safety requires that the NRC become involved with attempts to mitigate the adverse consequences of failures of this system.

The memo of August 8, 1980, also noted that a number of the items contained within recommendation 5 should be incorporated into the review of the responses to Bulletin 79-27. However, it does not appear that this actually happened. For example, an internal NRR memo dated September 18, 1980, stated, "The proposed Supplement [to Bulletin 79-27] does not address all aspects of the Crystal River event that are considered in NUREG-0667. These additional concerns will be addressed separately, rather than to change Bulletin 79-27 to include these considerations now."

In fact, rather than expanding the scope of that analysis, as previously discussed, the scope of the analysis of the responses to Bulletin 79-27 was progressively narrowed. The final review included a review to ensure that licensees had stated or clearly implied that they had conducted the evaluation required by the Bulletin and that a limited amount of information had been provided without any review of the actual information to verify the results of the analysis.

For recommendation 14, which discussed emergency procedures for loss of NNI and ICS, the conclusion was that Bulletin 79-27 required that this action be taken. The prioritization specifically stated that it was assumed that the procedures were in place and correct as a result of the actions required by Bulletin 79-27. The prioritization went on to state that this item was of such importance that the procedures should be reviewed by IE to verify that the equipment claimed to be available would indeed be available after an ICS or NNI malfunction. However, as discussed elsewhere, procedures for loss of ICS power were not prepared at Rancho Seco.

The prioritization also assigned a numerical priority to each recommendation. The priority assigned for these recommendations included:

<u>NUREG-0667</u> <u>Recommendation</u>	<u>Priority</u>
5	2
14	1

The definition of the priorities is:

Priority 1. Items should be scheduled and implementation begun as soon as possible. These items may require rescheduling of NRC staff and licensee/industry priorities and resources.

Priority 2. Items should be scheduled and implemented in accordance with existing priorities and resources.

The results of this prioritization were subsequently reviewed and an implementation plan was developed. An internal NRR memo dated March 6, 1981 noted that the ICS/NNI improvements were currently being implemented through related actions. The memo also noted that the high priority efforts (i.e., the Priority 1 recommendations) had largely been accomplished by the TMI Action Plan and through other requirements.

Recommendations 5(d), 5(f), and 5(h), described above, were deferred until resources and schedules could be established. For Recommendation 14 (emergency procedures for loss of NNI/ICS) the "Action Required" category was noted as being implemented through referenced requirements documents (i.e., "covered by Item 2 of IE Bulletin 79-27").

The March 6, 1981 memo provided some interesting insights into the staff's perceptions concerning the actions being taken as a result of the issue of NNI/ICS performance.

- o "In response to [BAW-1564 and the ORNL analysis], the NRC staff issued a letter on November 7, 1979 to all licensees of B&W-designed reactors requesting that the licensees provide their plans regarding these recommendations and their schedules for completing the work." [Emphasis added.]
- o "[T]he NRC issued Bulletin 79-27 on November 30, 1979 which required additional actions to be taken by licensees of all nuclear power plants with respect to the safety concerns related to control systems." [Emphasis added.]
- o Following the Crystal River event, "licensees with B&W-designed reactors were requested to complete three additional requirements" [Emphasis added.]
- o With respect to Recommendation 14 (plant-specific procedures concerning the loss of NNI/ICS), "we assume these procedures to be in place and correct when deciding that Recommendation 5 was not high priority..." [Emphasis added.]

A draft of NUREG-0667 was sent to SMUD for review and comment. However, there is no document that requires implementation by SMUD. In fact, other than routine document distribution, the final NUREG-0667, with its 22 recommendations, was never sent to SMUD for consideration of applicability.

Thus, it would appear that the staff believed that actions had been taken to reduce the vulnerability of B&W-designed plants to severe transients initiated by failures in the ICS and NNI, and to provide plant-specific procedures to allow the operators to efficiently and effectively mitigate the consequences of such events. However, at Rancho Seco, these "actions" included primarily the preparation of responses to the NRC that concluded that additional actions and additional procedures (e.g., a loss of ICS procedure) were not necessary.

In summary, Bulletin 79-27 states, "Prepare emergency procedures or review existing ones that will be used by control room operators ... upon loss of power to ... instrument and control systems." In addition, NUREG-0667 states, "Licensees should develop and implement promptly plant-specific procedures concerning the loss of NNI/ICS power." The staff has stated, "we assume these procedures to be in place and correct..." In fact, a procedure for loss of ICS power does not exist at Rancho Seco.

The staff initially (i.e., 1979/1980) had concerns about the transient response of B&W-designed reactors and the role of the ICS as an initiator of such transients. NRC performed an extensive study which made 22 recommendations on this

issue. However, it does not appear that these recommendations were sent to SMUD for action, or that the recommendations relevant to the December 26, 1985 incident were implemented at Rancho Seco.

It appears that the assumption was made that the more significant of these recommendations would be included in the review of SMUD's response to Bulletin 79-27. However, from the Team's discussions with staff members involved with that review, this assumption was not communicated to those reviewing Bulletin 79-27.

#### 7.1.6 March 19, 1984 Partial Loss of NNI at Rancho Seco

On March 19, 1984, a hydrogen explosion and fire occurred in the electrical generator at Rancho Seco while the plant was operating at 85 percent power. Following the explosion, the turbine was tripped manually from the control room, causing an immediate reactor trip. The fire was extinguished automatically by the area CO<sub>2</sub> system, and the plant was safely shut down. Twice within the next several hours, the plant experienced a partial loss of NNI power.

NRC staff reviewers went to the site to review the circumstances surrounding the hydrogen explosion, fire, and partial loss of NNI. Subsequently, some of these reviewers prepared a report on the visit and distributed it within the NRC on June 29, 1984. The report is very lengthy and includes an extensive discussion of the partial loss of NNI.

Among the conclusions contained in the report was that the "loss of NNI power event at Rancho Seco again demonstrated that the failure of non-safety related equipment at B&W plants has the potential to cause plant transients that challenge the operator's capability to mitigate the transient without resulting in overcooling or undercooling of the primary system." The report also noted that the event demonstrated the effectiveness of plant modifications implemented following the lightbulb incident.

The report went on to note that the March 19, 1984 loss of NNI was the result of a single failure of an inverter compounded by a separate undetected failure of the NNI power supply monitor due to set point drift. These failures caused the loss of redundant NNI power sources. The report noted that past efforts to improve the reliability of the NNI system focused on providing redundancy within the NNI power distribution system but that a number of loss of NNI power events have occurred subsequent to the modifications providing this redundancy. The report concluded that it may be appropriate to focus future efforts on preventing adverse ICS-induced transients, given a loss of NNI power.

The report stated that the ability of the Rancho Seco design to respond to loss of NNI events appeared to be marginally acceptable. It also noted that further review was necessary to: (1) determine whether the potential existed for NNI failures that can cause ICS induced transients, and (2) determine whether NNI/ICS modifications were warranted to reduce the severity of the transient and the resultant burden on the operators. The report recommended that this effort be included in the resolution of USI A-47 or be referred for further consideration within NRR.

The report also included a number of specific findings and recommendations that are relevant to the December 26, 1985 incident:

- o The majority of recommendations in NUREG-0667 for improving B&W NNI and ICS designs have not been resolved.
- o Based on the review of the March 19, 1984 loss of NNI at Rancho Seco, the need to resolve these items still exists.
- o The NUREG-0667 recommendations for improving B&W NNI and ICS designs should be reviewed to determine whether implementation should be required.

This report was one of a number of reports that were to form the basis for an overall NRR report on this event. The NRR overall report has not yet been completed and the report described above was not forwarded to SMUD.

Because of the generic aspects of the event, the staff met with the licensees for all B&W-designed plants to discuss the event. Subsequently, the staff sent, on September 4, 1984 a number of questions to the B&W Owners Group concerning the NNI.

In response to the September 4, 1984 letter, the B&W Owners Group submitted a letter dated January 11, 1985. Some of the questions and responses are noteworthy in the context of the December 26, 1985 incident:

"Does the ICS receive erroneous/false input signals on loss of NNI power?" The B&W Owners Group response stated that the loss of NNI power can result in erroneous or false input signals to the ICS. The response further stated that this will not necessarily result in adverse consequences. This conclusion does not appear to be consistent with the previous events where loss of NNI power has resulted in control system functions by the ICS that have resulted in significant plant transients (e.g., the lightbulb incident, the Crystal River event, the Oconee event).

In the questions asked by the staff and responses provided by the B&W Owners Group, we again see strong evidence of a narrow focus on the NNI. The questions, in general, do not refer directly to the ICS and only consider situations where loss of NNI power resulted in erroneous inputs to the ICS. As a result, the full significance of the loss of power to the ICS was not addressed. In a number of cases, if questions that now read "Can the loss on NNI..." were restated as "Can the loss of NNI or ICS..." the answers would be quite different. For example, Question E.3 asks, "Can the loss of NNI power cause the ICS to open turbine bypass valves or atmospheric dump valves?" The answer for Rancho Seco was "No." However, if the question were restated as "Can loss of NNI or ICS power...?" the answer, as demonstrated by the December 26, 1985 incident, would be "Yes." It is the understanding of the Team that the responses by the B&W Owners Group are still being evaluated by the staff.

The March 19, 1984 loss of NNI power at Rancho Seco again demonstrated that the failure of nonsafety-related equipment at B&W-designed plants has the potential to cause plant transients and to challenge the operators' capability to mitigate the transient without overcooling and undercooling of the primary system. However, despite the fact that this event occurred nearly 2 years ago, the December 26, 1985 incident demonstrates that effective actions have not been implemented by SMUD to resolve this situation.

### 7.1.7 USI A-47, "Safety Implications of Control Systems"

Throughout the review of the precursors to the December 26, 1985 incident, the Team found repeated references to Unresolved Safety Issue (USI) A-47, "Safety Implications of Control Systems." In a number of cases, the long-term implications of various issues concerning the Rancho Seco control system were referred to USI A-47. Thus, the Team reviewed USI A-47 to determine how these long-term implications had been included within the scope of the USI.

The most recent document describing USI A-47 is Revision 3 of the NRC Task Action Plan (TAP) dated March 1985, which notes that during plant licensing the staff reviewed the nonsafety-related control systems only to ensure that an adequate degree of separation and independence was provided between these systems and the safety-related systems, and that effects of the operation or failure of these systems were bounded by the accident analysis in the plant's Final Safety Analysis Report (FSAR).

Under USI A-47, detailed analysis was performed on one reference plant from each of the principal nuclear steam supply system (NSSS) suppliers (for B&W-designed plants, the reference plant was Oconee). The analysis was to verify the adequacy of the existing NRC criteria for control systems and to determine the need for control or protection system improvements. However, the TAP notes that developing generic resolutions based on plant-specific reviews has certain limitations.

For the purpose of justifying continued operation of the operating reactors, the TAP noted the prior work done as a result of BAW-1564 and Bulletin 79-27. However, for BAW-1564 the TAP did not recognize that the staff's resolution of the long-term issues had been referred to USI A-47. In reference to BAW-1564, the TAP noted that NRR had concluded that the B&W analysis showed that anticipated failures within the ICS were adequately mitigated by the plant safety systems and that B&W-designed plants were requested to evaluate the B&W recommendations and report their followup actions. Subsequently, the responses were reviewed and found acceptable. In addition, the TAP noted that for Bulletin 79-27, the licensees have indicated that corrective actions have been taken, including hardware changes and revised procedures where required.

The Team also reviewed the draft report on the resolution of USI A-47 in detail. The goal of USI A-47 as stated in this report included: (1) identify the nonsafety-related control system failures that could produce transients potentially more severe than those previously analyzed in the FSAR, (2) identify nonsafety-related control system failures that could adversely affect any assumed or anticipated operator action, (3) identify nonsafety-related control system failures that could cause Technical Specification Safety Limits to be exceeded, (4) identify nonsafety-related control system failures that could cause transients to occur at a frequency in excess of the values established for Abnormal Operational Transients, and (5) identify nonsafety-related control system failures that could cause frequent challenges to the protection systems. In addition, the draft report noted that an evaluation was made to assess the generic applicability of the review.

The draft report notes that a literature search of operating experience was conducted to identify those failures that could meet any of the criteria described above. Failures that met these selection criteria were considered to be safety significant. To determine generic applicability, the significant

transients analyzed for the reference plants were also evaluated to determine if the transients could occur at other plants, and if the transients analyzed for the reference plant represented a more severe or bounding transient.

The draft report noted that control systems on other plants were similar to the reference plant and/or the differences in the design were not significant enough to substantially alter the events of concern. The draft report lists a few plants whose designs vary significantly from the respective reference plants. None of the B&W-designed plants were listed as being different than the B&W reference plant. However, this is not consistent with a number of other references in the draft report that indicate that the control system designs vary considerably from plant to plant. For example, in the case of B&W-designed plants, the 721 design of the ICS at the reference plant is substantially different than the 820 design used at Rancho Seco.

From a review of the conclusions identified in the draft report for USI A-47, and from information acquired in interviews of the staff, it appears to the Team that there is an inconsistency between the stated objectives of this study, the work that was actually performed, and the draft conclusions that were reached. The initial scope included a broad range of issues, including events bounded by the FSAR analysis that are of high frequency. However, the conclusions reached for the reference B&W-designed plant identify only two transients that were considered to be of interest. Other control system failures were excluded from detailed analysis because it was determined that they were bounded by the FSAR analysis. The two events that were found to be of interest are: (1) initiation of overfeed and failure of the automatic feedwater pump trip system that would have terminated an overfill event, and (2) a loss of electrical power to various sections of the integrated feedwater control system, resulting in a feedwater underfeed condition that could lead to core overheating if proper operator action was not taken.

For Rancho Seco, the overfill event was determined to be acceptable because of SMUD's commitment to install a safety-grade overfill protection system as part of emergency feedwater initiation and control (EFIC) system. The report observes that Rancho Seco has committed to install this system by mid 1988. However, the report does not evaluate the existing control system at Rancho Seco, which does not include any automatic overfill protection, particularly in light of the long delays that have occurred in the installation of EFIC (see Section 7.2 for a more detailed discussion of EFIC).

In addition, although the analysis considered whether the events of concern for the reference plant were relevant to the other plants, the converse analysis was not performed. Thus, no analysis was performed to determine if there were events that could be significant at Rancho Seco that were not significant at the reference plant because of differences in design. For example, overcooling transients, such as occurred at Rancho Seco on December 26, 1985, would be excluded from the analysis performed by USI A-47 because at the reference plant such events would not have produced an overcooling transient that exceeded 100°F per hour.

While the scope of USI A-47 is broad, it appears that the actual analysis performed to date included only those events with a potential to be outside the design basis of the reference plant. Such events are rare and do not appear to address the substantive issues of frequent challenges of protection systems and



frequent abnormal operating transients such as those that resulted in the concerns identified in BAW-1564, Bulletin 79-27, and NUREG-0667. In addition, the analysis considered reference plants, and differences in plant design that could cause an event that was benign at the reference plant to be significant at another plant were not evaluated. Thus, the analysis to date is limited to design basis events at the reference plant. Therefore, it does not appear that the analysis performed under USI A-47 addresses all of the issues that had been deferred to it by Bulletin 79-27, BAW-1564, or NUREG-0667. Thus, results of the resolution of USI A-47 are of quite limited applicability to B&W-designed plants beyond the reference plant that was studied. The results are not directly applicable to most other B&W-designed plants, such as Rancho Seco, because of the differences in the design of the ICS.

## 7.2 Emergency Feedwater Initiation and Control (EFIC) System

This section describes the purpose of the emergency feedwater initiation and control (EFIC) system, describes the design of the system, discusses the significance of the absence of this system on the December 26, 1985 incident and describes the regulatory history of EFIC.

### 7.2.1 System Purpose

The requirement for a system such as EFIC arose initially out of the accident at Three Mile Island in March 1979. (See Regulatory History in Section 7.2.4.)

The primary purpose of the EFIC system is to provide automatic initiation of AFW and AFW flow indication with a safety-related Class 1E instrumentation system independent of the ICS and NNI systems. The system also fulfills several secondary purposes including providing one train of AFW that is diversely powered and independent of ac power, preventing overfill of the OTSGs (i.e., to provide automatic and reliable control of the AFW flow), and providing better control of paths of excessive steam flow that could decrease the time for OTSGs to boil dry (i.e., the ADVs).

### 7.2.2 System Description

The EFIC is designed as an independent safety-related Class 1E system. It is automatically initiated when any of the following plant conditions occur:

- o Loss of main feedwater flow (as indicated by the reactor power/MFW flow reactor trip signal)
- o Low water level in either OTSG
- o Loss of all four reactor coolant pumps
- o Low pressure in either OTSG
- o Emergency core cooling system (ECCS) actuation (Reactor Building pressure high or RCS pressure low)

Upon actuation, EFIC will control AFW to maintain water level in the OTSGs. EFIC has two features to minimize overfill and overcooling. First, if the level reaches 20 feet, MFW is automatically isolated by valve action. Second, the

rate at which AFW returns the water level to the setpoint is limited to 2 to 8 inches per minute (depending on OTSG pressure) by modulating the AFW flow control valves.

For main steamline or main feedline break protection, EFIC will automatically isolate MFW to the affected OTSG when its pressure falls to less than 600 psig. Additionally, EFIC includes a feed-only-good-generator AFW flow control.

EFIC also improves OTSG pressure control because the ADVs will be controlled only by EFIC and not by the ICS. It should be noted that the TBVs will remain under ICS control and the Rancho Seco plant design does not include main steam isolation valves (MSIVs). Thus, the EFIC design does not provide for isolation of undesirable flow through the TBVs.

### 7.2.3 Significance of the Absence of EFIC

The December 26, 1985 incident was initiated by a loss of dc power within the ICS. This caused the TBVs and ADVs to open to the mid-stroke position. In addition, AFW was automatically initiated when the MFW pumps discharge pressure went below the setpoint. Both AFW trains initiated and started pumping water into the OTSGs through AFW flow control valves that had failed to the mid-stroke position when the ICS lost dc power. This excessive AFW flow contributed significantly to the overcooling of the RCS.

If EFIC had been installed and operational at the time of the incident the immediate plant response would have been different. First, the TBVs would have opened to mid stroke, but the ADVs would not have opened. Thus the rate of steam removal would have been much slower allowing more time for operator action. Second, AFW would have initiated, but would not have injected until the OTSG level fell below the low-level limit. The AFW flow control valves would have then modulated to maintain OTSG level at the low level limit. As a result of this sequence, the plant would have cooled down in a more controlled manner after the TBVs were closed. In addition, when the steam pressure decreased to 600 psig (versus the 435 psig setpoint of the MSFL system), MFW would have isolated. This action would have prevented the flow into the OTSGs from the condensate pumps. Thus, there would not have been any overflow of the OTSGs and less overcooling of the RCS.

In summary, had EFIC been installed, the overcooling event of December 26, 1985 would have been much less severe and probably would not have exceeded the Technical Specifications limit of 100°F in an hour.

### 7.2.4 Regulatory History of the EFIC System

The design concept for the EFIC system originated from the NRC's TMI Short Term Lessons Learned (NUREG-0578) requirement issued in 1979 for automatic AFW initiation independent of the ICS. Since then, the EFIC system was expanded to satisfy a number of related requirements.

#### 7.2.4.1 TMI Requirement II.E.1.2, AFW Automatic Initiation and Flow Indication

This section describes the NRC requirements, how SMUD has responded to the requirements, and the schedule for implementation.

NRC's "Short Term Lessons Learned From TMI," (NUREG-0578) item 2.1.7, which later became TMI Action Item II.E.1.2, required actions aimed at improving AFW system reliability. One of the requirements was that the AFW system should be automatically initiated, independent of the ICS. The intent of this requirement was that AFW flow be initiated automatically and completely for any situation for which the operation of the AFW was necessary for safety. The AFW initiation system was not required to be fully safety grade initially, but it was required to meet certain safety-grade requirements, such as the single - failure criterion. The requirement was that eventually the AFW initiation system would be upgraded to fully safety related.

SMUD first responded to requirement 2.1.7 with a letter dated October 18, 1979 in which they committed to install a safety-grade AFW initiation and control system, independent of ICS, during their 1981 refueling outage.

NRC's "Clarification of TMI Action Plan Requirements," (NUREG-0737) included these requirements as item II.E.1.2, and established a required implementation schedule. The modifications were to be installed by July 1981.

#### 7.2.4.2 TMI Requirement II.E.1.1, AFW System Upgrade

This section describes the requirements for AFW system upgrade, how SMUD has responded to that requirement, and the schedule for implementation.

NUREG-0737 item II.E.1.1 required licensees to perform the following:

1. Analyze AFW system reliability using event-tree and fault-tree logic techniques, with particular emphasis on common-cause and single-point failures.
2. Review the AFW system against the NRC Standard Revised Plan section 10.4.9 and the associated Branch Technical Position ASB 10-1.
3. Re-evaluate the AFW flow rate design basis and criteria.

SMUD submitted the AFW reliability analysis by letter dated December 17, 1979. The NRC requested additional information about this analysis and the other two requirements, by letter dated February 26, 1980. One of the NRC questions concerned the fact that the loss of NNI/ICS power was not identified by SMUD as a single failure source for the AFW system. SMUD provided partial responses to this question in letters dated March 18, April 14, and May 14, 1980.

The May 14, 1980 response addressed the issue of loss of NNI/ICS power, stating that the power sources are battery-backed inverters that were assumed to be available under all operating conditions. The response goes on to state that this assumption was required by the NRC, to maintain consistency with previous analyses. The NRC found this response acceptable.

As a result of this analysis, SMUD identified a number of AFW system upgrades that were needed to comply with II.E.1.1.

### 7.2.4.3 Introduction of EFIC

At the request of the B&W-designed plant licensees, the NRC staff attended a presentation on September 4, 1980 regarding an extensive upgrade of the AFW systems which was to be undertaken generically. At this meeting, B&W and the licensees introduced the emergency feedwater initiation and control (EFIC) system as the consolidated answer to many NRC requirements. EFIC would encompass extensive AFW upgrades including those from a number of ongoing NRC concerns. The features of EFIC that are relevant to the December 26, 1985 incident arise from the reliability analyses (i.e., TMI action item II.E.1.1), the automatic AFW initiation requirement (i.e., TMI action item II.E.1.2), and other safety-related requirements. EFIC also included an automatic AFW control system which addressed the OTSG overfill and RCS overcooling recommendations arising from NUREG-0667, and the concern regarding the spurious opening of ADVs upon loss of ICS power.

The licensees indicated that EFIC would be installed at a number of B&W-designed plants, including Rancho Seco. Arkansas Nuclear One, Unit 1 (ANO-1) would be the "lead plant" for the EFIC system, with submission of the conceptual design for NRC review by October 1980, installation at ANO-1 in early 1982, and installation at the last B&W-designed plant by late 1982.

Thus, as described in Section 7.2.2, the EFIC system proposed by SMUD in September 1980 would have included the following features that are relevant to the December 26, 1985 incident:

- The ADVs and AFW (ICS) flow control valves would be controlled by the safety-grade EFIC system and would no longer open on loss of ICS dc power.
- A safety-grade overfill protection system would have been installed that would have prevented flow to the OTSGs from the condensate pumps.

Based upon the design information provided by SMUD in their November 17, 1980 letter, in January 1981 the NRC staff approved the preliminary design of the EFIC system as the response to Item II.E.1.2 for Rancho Seco.

SMUD submitted a letter dated October 22, 1982 stating that the AFW automatic initiation system (which was now part of EFIC) would be installed during the 1983 refueling outage, then scheduled for January 1983. In early 1983, the NRC determined that the safety upgrades to the AFW system, including II.E.1.2, were sufficiently important that the most recent installation schedule should be required by an NRC Order. NRC issued this Order on March 14, 1983 and required that SMUD complete installation of the AFW automatic initiation system as scheduled during the 1983 refueling outage. The Order also mentioned that the safety grade AFW flow control system would not be installed until 1984.

SMUD's April 28, 1983 letter states that the installation schedule for EFIC had slipped until a refueling outage in 1986. The reason given was that EFIC was closely related to both the ongoing Detailed Control Room Design Review and the implementation of Regulatory Guide 1.97, Revision 2 (post-accident monitoring instrumentation). The letter states that this schedule change would not affect the part of the system dealing with the item II.E.1.2 (i.e., the AFW automatic initiation system).

Apparently SMUD had now concluded that the EFIC system was no longer required to meet the commitment to provide an AFW automatic initiation system (i.e., II.E.1.2) because SMUD had improved the AFW initiation system such that the AFW system would be initiated on SFAS. However, SMUD did not document this alternative response to the requirements of II.E.1.2, and did not submit information to the NRC that explicitly stated that the alternate design would be used to satisfy the requirements in II.E.1.2, instead of the previously approved EFIC system. In addition, they did not submit the alternate design to the NRC for review and approval.

In the alternate design (i.e., non-EFIC), the AFW system would be initiated automatically under some accident conditions (i.e., RCS low pressure, containment building high pressure), but would not initiate under all conditions for which AFW initiation is necessary (e.g., loss of MFW). Thus, this alternate design may not have complied with the requirements of item II.E.1.2 as described earlier.

Thus, the fact that some automatic AFW initiation had been provided, combined with the lack of specificity of the intent of the original NRC requirement, was sufficient for SMUD to conclude that they had complied with the requirements of this item. Being under an NRC Order to implement item II.E.1.2 by a specified date, and facing the schedule slippages to install EFIC, which they originally committed to in their response to II.E.1.2, SMUD concluded that the earlier AFW initiation modifications had complied with the requirements of the Order, thus allowing them to avoid an extended plant outage because of a failure to comply with the NRC Order.

Apparently, the majority of the NRC staff associated with this issue was not aware that the NRC-approved design for Item II.E.1.2 (i.e., EFIC) had not been installed at Rancho Seco. However, following the October 1985 overcooling event at Rancho Seco, some NRC staff members realized that EFIC had not been installed at Rancho Seco and believed that SMUD had not conformed with the March 1983 Order. They questioned the prudence of authorizing plant restart in view of their perception that SMUD was in violation of the NRC Order. The Team understands that the question of whether the AFW initiation system installed at Rancho Seco complies with the requirements of the March 1983 Order (i.e., II.E.1.2) and whether SMUD violated the March 1983 Order by not installing EFIC is still under review by the NRC staff.

As part of the proposed "Living Schedule" program, SMUD has scheduled the EFIC system to be installed in mid-1988.

In summary, the staff was led to believe that the EFIC system would be installed in 1984 in response to a number of NRC requirements, including II.E.1.2. Apparently SMUD decided to install an alternate system in response to II.E.1.2. SMUD's intent to satisfy II.E.1.2 with this alternate design was not made clear to the NRC staff, was not approved by the staff, and may not have complied with the requirements of II.E.1.2. As a result, the EFIC system, some features of which would have reduced the severity of the December 26, 1985 incident, has not yet been installed at Rancho Seco.

Table 7.1 Chronology of Precursor Events and Related Actions

March 20, 1978	Rancho Seco loss of NNI event (the lightbulb incident)
January 5, 1979	Rancho Seco loss of ICS event.
March 28, 1979	TMI accident.
August 1979	BAW-1564 "Integrated Control System Reliability Analysis."
November 10, 1979	Oconee loss of NNI/ICS event.
November 30, 1979	IE Bulletin 79-27 "Loss of Non-class-1E-instrumentation and Control Power System Bus During Operation."
January 21, 1980	ORNL review of BAW-1564.
January 21, 1980	Rancho Seco comments on BAW-1564.
February 20, 1980	Rancho Seco response to Bulletin 79-27.
February 26, 1980	Crystal River loss of NNI event.
March 6, 1980	Letter sent to Rancho Seco requiring information concerning the Crystal River event.
March 12, 1980	Rancho Seco response to the Crystal River letter.
March 6, 1980	NRC letter concerning the Crystal River event.
March 1980	NRC Order concerning NNI improvements.
May 1980	Region close-out of Item 2 of Bulletin 79-27.
May 1980	NUREG-0667, "Transient Response of Babcock & Wilcox Design Reactors."
September 1980	A technical branch in NRR concludes that Rancho Seco's response to Bulletin 79-27 is inadequate. A technical branch in NRR prepares the first draft supplement of Bulletin 79-27.
January 1981	The technical branch in NRR prepares the second draft supplement to Bulletin 79-27.
June 26, 1981	NRR concludes that Rancho Seco's response to Bulletin 79-27 is inadequate. Third draft supplement to Bulletin 79-27 is prepared.
June 3, 1981	Implementation Plan for NUREG-0667 ICS-related actions to be implemented under Bulletin 79-27.

Table 7.1 Chronology of Precursor Events and Related Actions (Continued)

---

January 13, 1982	NRR closes II.K.2.9. (BAW-1564) for Rancho Seco Long-term issues deferred to USI A-47.
June 1, 1982	NRR concludes that Rancho Seco's response to Bulletin 79-27 is acceptable. Long-term issues deferred to USI A-47
March 19, 1984	Rancho Seco partial loss of NNI event.
June 29, 1984	Rancho Seco partial loss of NNI report.
September 28, 1984	NRR closes II.E.5.2. based on publication of NUREG-0667.

---





## 8 SAFETY SIGNIFICANCE OF THE INCIDENT

### 8.1 Introduction

In order to assess the safety significance of the incident from the perspective of the potential impact on public health and safety, the Team compared its consequences to the analysis of accidents and abnormal operational transients in the Rancho Seco Final Safety Analysis Report (FSAR), and to the pressurized thermal shock (PTS) analysis of B&W-designed reactors. In addition, the Team considered the expected frequency of such events and compared this event to "the lightbulb incident" at Rancho Seco in 1978. Finally, the Team evaluated whether the event might have been more significant under alternative scenarios of delayed operator action.

A feedwater transient, if not effectively controlled, may develop into two scenarios (1) total loss of feedwater, or (2) excessive feedwater. Both can have significant consequences if actions to ensure prompt and effective recovery are not taken. The December 26, 1985 incident is an example of an excessive feedwater event which resulted in an overcooling incident.

### 8.2 Pressurized Thermal Shock

When a reactor trips, the preferred heat removal path is through the once-through steam generators (OTSGs), where reactor coolant heat is transferred to the feedwater. A loss of feedwater, if not recovered, can result in reduced heat transfer from the reactor coolant, ultimately leading to overheating the reactor core and possible fuel damage. Unlike a loss of feedwater, the December 26, 1985 incident (following the reactor trip) involved excessive feedwater flow to the OTSGs combined with excessive steam flow through the turbine bypass valves (TBVs) and atmospheric dump valves (ADVs), a condition which results in excessive heat transfer from the reactor coolant that causes the temperature of the reactor coolant to drop. The colder reactor coolant also reduces the temperature of the reactor pressure vessel. If the vessel temperature drops low enough, and the reactor coolant system (RCS) pressure is high enough, the vessel can exhibit brittle behavior rather than the desired ductile behavior.

The concern about this combination of a rapid temperature drop and high pressure for pressurized water reactors is called pressurized thermal shock (PTS). The NRC staff's analyses and evaluation of this issue are documented in SECY-82-465, "Pressurized Thermal Shock (PTS)," dated November 23, 1982 which forms the analytical basis for the NRC's PTS requirements in 10 CFR 50.61. The important parameters in an overcooling event are reactor coolant pressure and temperature, flow rates of systems which transfer heat to and from the reactor coolant, and the reactor vessel ductility characteristics (reference nil ductility temperature).

In considering vessel ductility, important parameters vary from vessel to vessel. They include the unirradiated reference nil ductility temperature, the amount of neutron irradiation that has accumulated, and the composition of the

steel (e.g., copper and nickel content). In this regard, 10 CFR 50 Appendix G specifies basic fracture toughness requirements for ferritic (steel) materials of pressure-retaining components of the RCS pressure boundary. However, 10 CFR 50.61, addresses the one additional factor important to the severity of an overcooling event which places it in the PTS range: the rate of cooldown. The rate of cooldown of the reactor vessel influences the stresses created in the steel. A rapid cooldown of the reactor vessel internal surface causes a temperature variation through the vessel wall. This temperature variation produces a thermal stress with a maximum tensile stress at the inside surface of the vessel whose magnitude depends on the cooldown rate. The total stress on the vessel includes the thermal stress as well as the pressure stress from the RCS pressure. Thus, cooldown rate is important, and specific limiting values for this rate are specified in a plant's Technical Specifications. Typically, plants limit their cooldown rates to less than 100°F/hr from temperatures above about 500°F. For B&W-designed plants (including Rancho Seco) B&W has specified a combination of RCS pressure and temperature ranges which it recommends licensees avoid. The Team has defined this as "the PTS region" as shown in Figure 4.6.

### 8.3 Analyses

#### 8.3.1 Comparison with the "Lightbulb Incident"

A previous, and more severe, overcooling event occurred at Rancho Seco in 1978 and was successfully mitigated (the so-called lightbulb incident). A temperature-time comparison of that incident with the December 26, 1985 incident is provided in Figure 8.1 and helps to provide perspective on the significance of the December 26, 1985 incident. In the 1978 event, the lowest RCS temperature reached was 295°F, almost 100°F lower than in the December 26, 1985 incident. The reference nil ductility temperature of the vessel ( $RT_{NDT}$ ) in 1978 was about 152°F. Also, during the lightbulb incident reactor coolant pressure was maintained at a high level (about 2,000 psig) throughout the cooldown, which lasted over an hour. In contrast, during the December 26, 1985 incident, pressure was significantly lower (from 1,000 to 1,600 psig) and the cooldown shorter (25 minutes) and less severe; however,  $RT_{NDT}$  was somewhat higher because of the greater accumulated neutron fluence (about 202°F using the NRC staff's most current calculational method in Draft Regulatory Guide 1.99, Rev. 2. SMUD has calculated 217°F using the method in 10 CFR 50.61).

The December 26, 1985 cooldown was initially more rapid than the 1978 event. In about 7 minutes from the initial loss of ICS power, the RCS temperature dropped more than 100°F and the pressure dropped more than 1,000 psi. Eventually an RCS temperature of 386°F was reached at a pressure of 1413 psi. The cooldown stopped when ICS power was restored 26 minutes after the transient began. The RCS cooled down 180°F in this 26-minute period.

#### 8.3.2 Generic PTS Analyses

The analyses performed in SECY-82-465 can be used to estimate how close the December 26, 1985 incident came to a condition where brittle fracture of the reactor vessel would be a serious concern. The likelihood of crack initiation in a reactor vessel which experiences a severe cooldown depends on several parameters, including a critical RCS pressure and temperature. Figure 8.2 shows a set of critical temperature vs. pressure curves for different cooldown

rate-time constants, beta. If the final RCS temperature ( $T_f$ ) drops below the reference nil ductility temperature ( $RT_{NDT}$ ) at high pressure (upper left side of the figure), the initiation and/or propagation of cracks can take place in the vessel wall. The overcooling events at Rancho Seco which occurred on December 26, 1985 and March 20, 1978 are shown for comparison on Figure 8.2. For both transients, beta was approximately 0.05 to 0.1  $\text{min}^{-1}$ . For the cooldown which occurred on December 26, 1985, Figure 8.2 indicates that the critical RCS temperature was approximately 170°F. That is, the RCS temperature would have had to rapidly drop another 215°F (i.e., to an RCS temperature of 170°F) while maintaining pressure around 1400 psi to have seriously threatened reactor vessel integrity.

A report prepared by the B&W Owner's Group, "B&W Owners Group Probabilistic Evaluation of Pressurized Thermal Shock Phase 1 Report," BAW-1791, dated June, 1983, analyzes overcooling transients due to various initiators, including a loss of ICS power for a B&W "generic plant configuration." The generic configuration selected was purported to be "biased toward the conservative side" with "comments about the configuration features where some differences exist from plant to plant ... interspersed throughout." The generic configuration includes the new emergency feedwater initiation and control (EFIC) system. At the time of the BAW-1791 analysis, no plant had EFIC installed and nearly 3 years later only two plants (ANO-1 and Crystal River 3) have installed EFIC. The report asserts that "the ICS is virtually the same from plant to plant," and that "the ICS control functions important to PTS (pressurized thermal shock) are performed by the following components":

- o Main flow control valves of the main feedwater (MFW) system (and associated MFW stop valves),
- o Startup MFW flow control valves,
- o Main feedwater pumps, and
- o Turbine bypass valves.

The report also draws the general conclusion that failure of ICS power supplies can cause the TBV and MFW flow control valves to fail 50 percent open, a condition considered to be a common-cause failure.

Because EFIC is not yet installed at Rancho Seco, the following additional ICS control functions are also important to PTS:

- o Auxiliary feedwater (AFW) (ICS) flow control valves, and
- o Atmospheric dump valves.

Thus, for Rancho Seco, the general conclusion in BAW-1791 regarding common-cause failure does not include the AFW (ICS) flow control valves and ADVs failing to the 50 percent open position on loss of ICS power. While the above description and corresponding analyses may characterize a generic plant, they do not appear to be conservative for the Rancho Seco design as it currently exists.

A comparison of the results of the BAW-1791 analysis and the December 26, 1985 incident is shown in Figure 8.3. The curve for the December 26, 1985 incident is somewhat above the other curves, perhaps because the actual RCS cold leg temperature data are plotted for Rancho Seco, whereas the B&W report analyses assume an initial temperature of 550°F in the vessel downcomer near the belt-

line welds. Thus, the December 26, 1985 incident appears to be comparable to these "stylized" curves developed by the B&W Owner's Group. This comparability may be due at least in part to the prompt operator actions during the December 26, 1985 incident compensating for the nonconservative aspects of the analysis described above. The B&W Owner's Group analysis depicted in Figure 8.3 for a generic configuration predicts that the transient analyzed (with operator action after 15 minutes) has a very high probability of occurrence: about  $4 \times 10^{-2}$ /reactor-yr. If it were applicable to all eight B&W-designed operating reactors, such a transient could occur at some plant approximately every 3 years. Thus, it would appear that this analysis predicts that events comparable to the December 26, 1985 incident would occur approximately once each third year even if EFIC is installed at all B&W-designed plants. The report also notes that only one B&W plant has the correct combination of components that cause the transient frequencies to be very high. The Team deduced that that plant was Rancho Seco.

It should be pointed out that the same report (BAW-1791) describes analyses for another rapid transient caused by a different initiator which also is predicted to have a high probability (see Figure 6.8 of BAW-1791). This transient could be caused by a small steamline break (or break-equivalent) on two loops with AFW to both OTSGs continuing. The resulting overcooling transient is predicted by BAW-1791 to be even more rapid than the December 26, 1985 incident and to have a probability of occurrence of  $1.3 \times 10^{-2}$ /reactor-yr. Based on the generic analysis, the probability associated with this transient is sufficiently high that this transient, which includes a more rapid cooldown than the December 26, 1985 overcooling incident, should be expected to occur during the life of B&W plants.

### 8.3.3 FSAR Accident Analysis

To determine if the licensing basis for Rancho Seco considered accidents that bounded the December 26, 1985 incident, the Team reviewed the FSAR analyses for Rancho Seco. The FSAR analyses are not as applicable to the December 26, 1985 incident as the generic PTS analyses. This appears to be a general situation applicable to most pressurized water reactors (PWRs) in the U.S. for the reason stated in SECY-82-465:

Such analyses [Safety Analysis Reports (SARs) in support of license applications] tend not to be of much help in evaluations of PTS. Many of the assumptions in such analyses were developed and accepted for licensing purposes without regard to PTS concerns. While SAR analyses appear to be appropriately conservative for calculations of reactor core thermal performance, PTS evaluations are most usefully performed using best-estimate calculations of pressure and temperature behavior. In addition, some potential event sequences that are not generally analyzed in detail in Safety Analysis Reports, because their consequences for core cooling are bounded by the design-basis event analyses, can be of greater significance for PTS evaluations.

The FSAR transient and accident analyses for Rancho Seco does not address the loss of ICS power. The December 26, 1985 incident involved open TBVs and ADVs which are equivalent to small main steamline breaks on both loops. Although the FSAR analysis does mention a small main steam line break, it asserts that this transient is bounded by the large main steam line break analysis. The main

steam line break is analyzed in Chapter 14 of the FSAR. That analysis seems to bound the cooldown rate and the radioactivity release from primary coolant leakage. However, it does not bound the lower temperature which can be reached by the RCS and vessel. The FSAR main steam line break analysis is concerned with the reactor's return to criticality due to extremely rapid cooling (most analyses consider only the first 100 seconds following the break).

In addition, there appear to be some inconsistencies in the analysis. For example, the analysis states that it assumes no ICS contribution. However, the analysis provides for TBVs and ADVs to automatically open and close and for the cooldown ultimately to be terminated by AFW (ICS) flow control valves automatically controlling steam generator level. All of these valves are controlled by the ICS. It appears that if they had not taken credit for ICS, the transient would be more severe. In another example, small steam line failures are stated to be encompassed by the larger steam line break analysis. While this may be true for reactor core thermal performance analyses, it is probably not the case for PTS analyses because the lowest RCS temperature that can be reached at Rancho Seco does not appear to be bounded by the large steam line break analysis.

In summary, it is not clear that the overcooling transient was within the Final Safety Analysis Report (FSAR) analysis of the Rancho Seco plant. The most comparable analysis is for the cooldown due to a main steam line break. However, this analysis includes only 100 seconds of the transient. In addition, the Rancho Seco FSAR analysis of main steam line break appears to be flawed and nonconservative in that it assumes that the nonsafety-related ICS operates successfully to mitigate the consequences of the accident. Finally, the generic B&W PTS analysis (BAW-1791) is not directly applicable to Rancho Seco because it assumes that the EFIC system is installed.

#### 8.3.4 Consequences of the Incident Under Alternate Conditions

In reviewing licensee safety analyses, the NRC staff conservatively assumes that no operator actions are taken in the control room for 10 minutes. If no operator actions of any kind had been taken for 10 minutes after the loss of ICS power at Rancho Seco, the following scenario might be expected:

The TBVs and ADVs would have remained open, steam generator pressure would rapidly drop below the 435 psi setpoint (about 4 minutes after reactor trip), and the main steamline failure logic (MSFL) would isolate MFW. However, AFW flow would continue throughout the transient but at a much higher effective flow rate because (a) the AFW safety features actuation system (SFAS) flow control valves would remain fully open, and (b) no operator actions would have been taken locally to close the AFW (ICS) flow control valves. Both OTSGs would be close to overflowing after 10 minutes, if they had not already overflowed.

On the primary side, no pressurizer sprays or high pressure injection (HPI) would operate until the SFAS signal had been received, which would probably occur about the same time that it actually occurred. Makeup and letdown would be isolated by the SFAS, no throttling of HPI would be done, and RCS pressure would continue decreasing until HPI flow reversed the pressure decrease. During this time the pressurizer would empty and a steam bubble could form in the upper reactor vessel. RCS temperature would rapidly drop to around 400°F after 10 minutes and continue dropping at about 15°F per minute. Meanwhile,

RCS pressure would be increasing towards the pilot operated relief valve (PORV) setpoint (2450 psi).

In another hypothetical scenario, the event proceeds, as it actually did, for 26 minutes, but ICS power is not recovered and no further actions are taken by the operators. Under these circumstances, calculations indicate that the RCS could have approached the critical area in Figure 8.2 in about another hour and a half.

It is unrealistic to assume that operators will do nothing for 10 minutes. During the December 26, 1985 incident, the operators were already taking actions in the control room within the first 15 seconds after loss of ICS power. Operator actions outside the control room began to have an impact on the course of the incident within 9 minutes following the reactor trip. Therefore, the scenarios above are considered highly unlikely.

The December 26, 1985 overcooling incident does not appear to have seriously threatened the integrity of the Rancho Seco reactor vessel. However, the plant has had a number of overcooling incidents in its 12-year operating history. Each time this occurs the potential exists for additional operator errors and equipment failures that might exacerbate the event and seriously threaten reactor integrity. Thus, the significance of this incident lies in the fact that under alternate scenarios more serious consequences could occur.

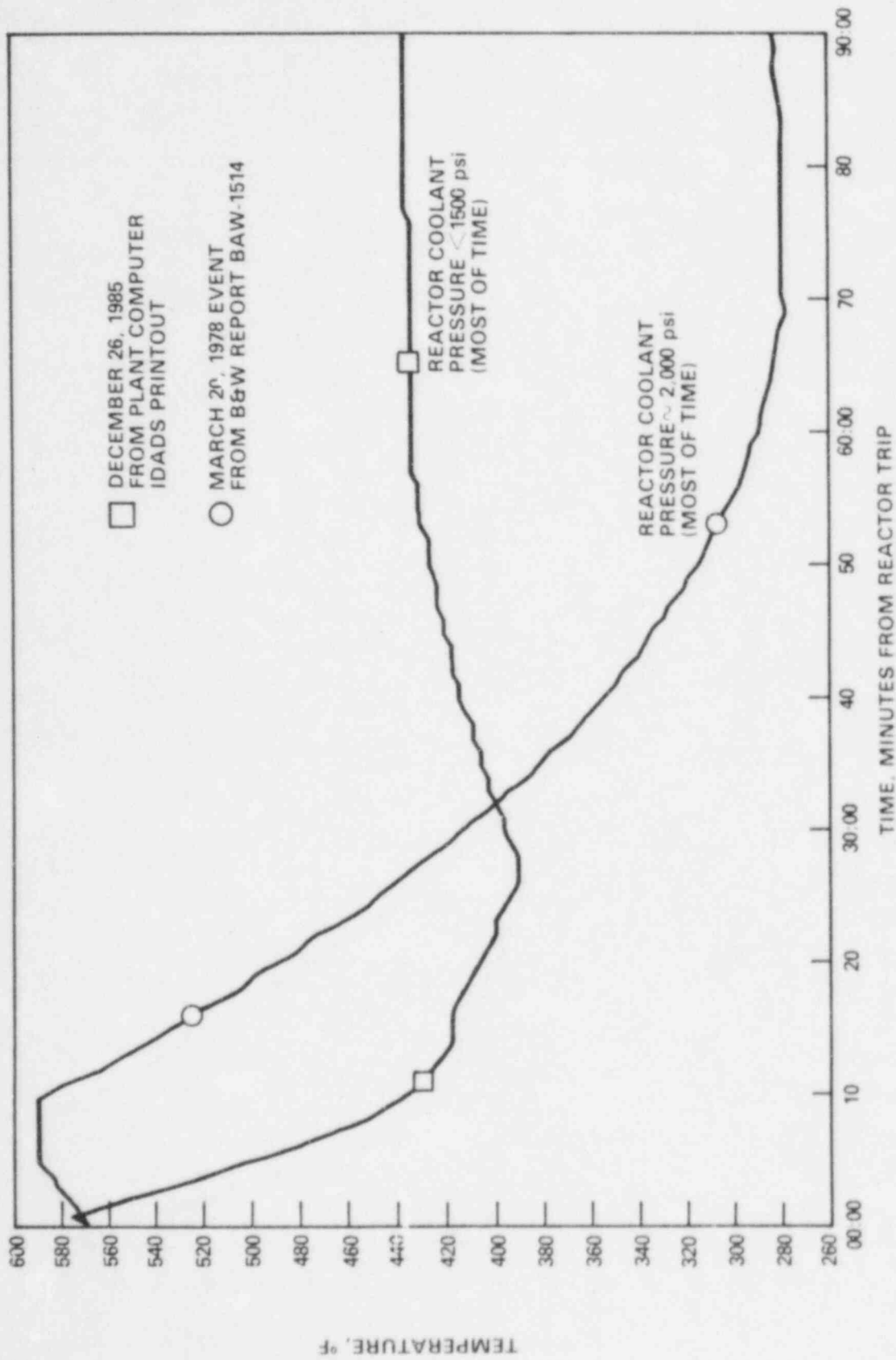


Figure 8.1 Overcooling incidents at Rancho Seco

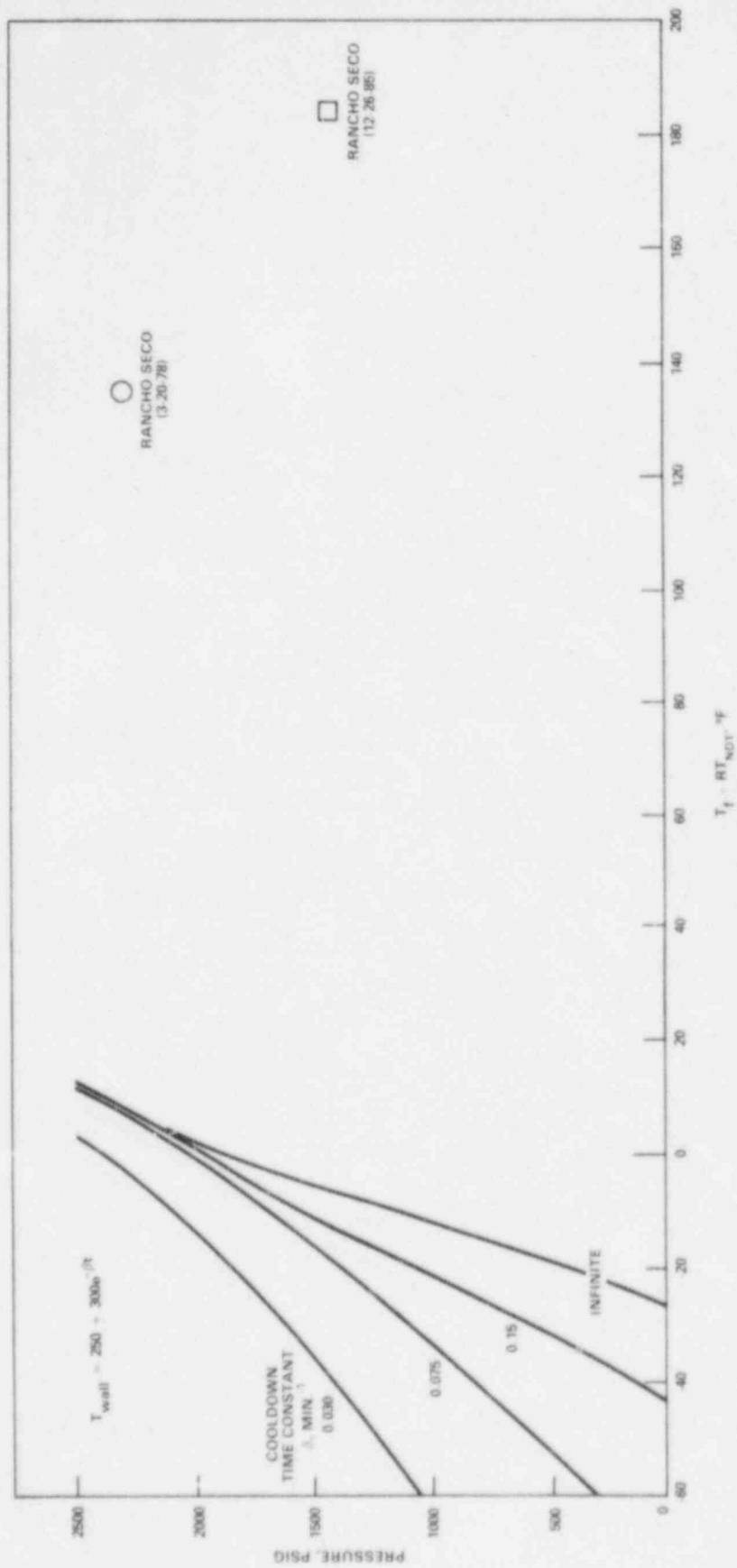


Figure 8.2 Critical values of pressure and  $T_f - RT_{NDT}$  for crack initiation in reactor vessels



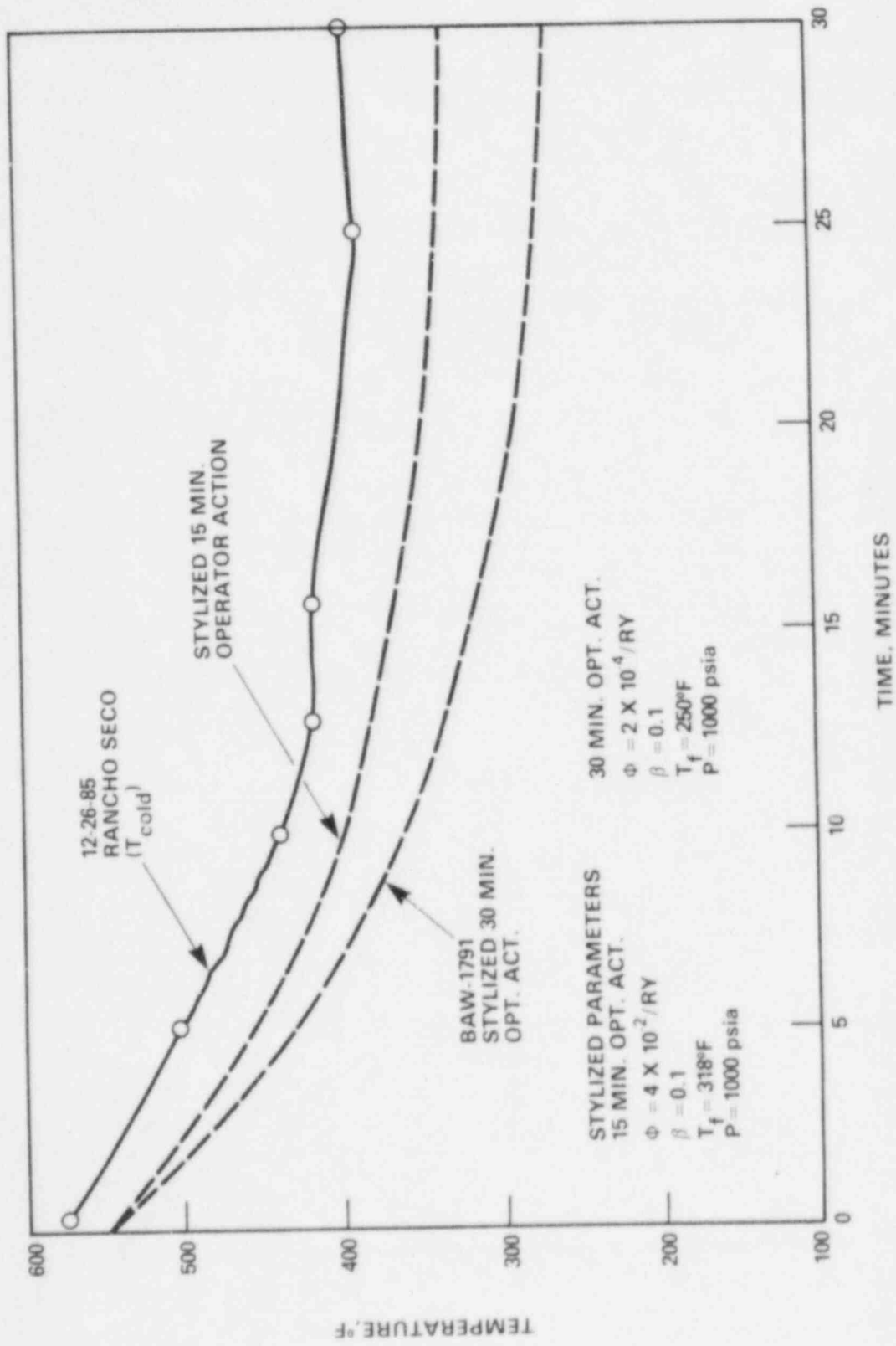


Table 8.3 Temperature versus time--ICS power supply failure with feedwater to both steam generators

## 9 ADDITIONAL ISSUES

In the course of its investigation, the Team learned about the issues discussed in this section. Although these findings are incidental to the Team's major findings, they were a part of the investigation and may be of regulatory significance.

### 9.1 Main Steam Line Failure Logic System

This section discusses the purpose and performance of the main steamline failure logic (MSFL), provides a description of the system and its safety classification, and discusses its dependency on the integrated control system (ICS).

#### 9.1.1 Purpose of the MSFL System

In the event of a failure of the main steam line, isolating the affected once-through steam generator (OTSG) is an essential safety function. Isolating the OTSG consists of blocking both the main feedwater flow to the OTSG and the main steam flow from the OTSG.

#### 9.1.2 Description of MSFL System

The Rancho Seco plant does not have main steam isolation valves (MSIVs). Therefore, the plant depends upon the turbine stop valves to isolate steam flow from the OTSGs. The automatic closure of the turbine stop valves is initiated by the reactor trip signal.

The isolation of main feedwater (MFW) is accomplished by the automatic closure of three valves in each main feedwater line: the main MFW flow control valve, the MFW stop valve, and the startup MFW flow control valve (which is located in parallel around the other two valves). If the two flow control valves are fully closed and the leakage is not excessive, the safety function of isolating MFW flow is completed. The flow control valves are air-operated and fast acting but may be subject to significant leakage. The slower MFW stop valve is motor-operated but typically allows less leakage. The system provided to shut the flow control valves is the MSFL and is discussed below. The isolating signal for the MFW stop valve is provided by the ICS. The combination of the main MFW flow and stop valves may meet the single-failure criterion; the single startup MFW flow control valve may not.

The MSFL detects excessive steam flow (indirectly) via pressure switches on the steam header downstream of each OTSG. Two fully redundant trains are provided and consist of sensing elements, logics, and actuated devices. The successful operation of either train is sufficient to close both of the main and startup MFW flow control valves for the associated OTSG. The two pressure switches within each train are configured in a 2-out-of-2 logic arrangement. When the logic is satisfied, the train will operate solenoid-operated valves which block the control air and vent the air-operated flow control valves. The MSFL is dc powered and must energize to actuate.

The normal flow overlap control for the MFW valves is provided by the ICS. Part of this scheme is that when the startup MFW flow control valve is open less than 20 percent, the MFW stop valve is automatically closed. A position switch on the startup MFW flow control valve provides the input signal to the ICS. Relays within the ICS then cause the stop valve to close. This feature is also used to complete the MSFL safety function (i.e., when the MSFL closes the startup MFW flow control valve, the ICS closes the motor-operated stop valve).

### 9.1.3 Safety Classification

The normal practice in the nuclear industry is that a system that performs an essential safety function must be classified as safety related so that the appropriate requirements and attention can be assumed. Generally, credit is taken in the Final Safety Analysis Report (FSAR) accident analysis only for systems that are classified as safety related.

Section 14.2.2.1 of the Rancho Seco FSAR addresses the postulated steamline break accident and takes credit for the successful operation of the MSFL. The FSAR assumes that closure of the MFW flow control valves will be completed automatically at 22.0 seconds, which in turn will be followed by closure of the MFW stop valve. The analysis goes on to assume that the subsequent contribution to the cooldown of the RCS from the MFW system is limited to that water inventory downstream of the valves.

During the Team's investigation of the December 26, 1985 incident, SMUD stated that the MSFL is not considered to be a safety-related system by the plant staff. Recently, in conformance with the new NRC equipment qualification rule (i.e., 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 the containment building). Special quality assurance procedures are now in force for these switches so as to preserve their "qualified" status. SMUD personnel stated that other components of the MSFL were purchased as "qualified" also. However, they went on to say that for maintenance purposes, the MSFL is listed as a nonsafety-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 MSFL 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 nonsafety-related ICS to close the MFW stop valve, and thereby assure that the safety function is accomplished in a single-failure-proof manner and that the leakage flow is not excessive.

## 9.2 AC Power Dependency of the AFW System

This section discusses the extent to which the auxiliary feedwater (AFW) system depends upon ac power to perform its safety function.

As shown in Figure 3.8, the AFW system at Rancho Seco consists of two full capacity trains. The A AFW pump is motor driven and would be automatically

sequenced onto the emergency diesel generator. The B AFW pump is dual-driven, having both a steam turbine and an electric motor on a common drive shaft. Upon system actuation, the steam turbine drive is activated automatically; the electric motor for this pump remains in standby and could be activated manually if needed. However, emergency power to the motor is not readily accessible. A hard-wired interlock prohibits the motor for the dual-drive pump from starting if the output breaker for the associated emergency diesel generator is closed. A key-lock override switch is provided for this interlock, but overloading the diesel generator may occur unless the load on the generator is less than 1900 kW when this override is used, a situation (i.e., a load less than 1900 kW) that is not likely in the first minutes after an accident.

The degree to which the AFW system is dependent on ac power to perform its safety function involves the valves in the AFW train. The steam admission valve for the AFW pump turbine (FV-30801) is a normally closed motor-operated valve, operated by dc power. Immediately upstream of this valve are two steam supply/isolation valves (HV-20569 and HV-20596), one from each main steam line. These valves are motor operated and require ac power. They are normally open but are not locked or "sealed" in this position; but, valve position indication and "valve not open" alarms are provided in the control room.

Two parallel flow control valves are associated with the turbine-driven AFW train. The AFW(SFAS) flow control valve (SFV-20577), is classified by SMUD as "safety related" and is opened by the SFAS. This is a normally closed motor-operated valve that requires ac power. As a motor-operated valve, it will remain in the "as is" position upon loss of power. Therefore, if offsite (ac) power is not available, this AFW(SFAS) flow control valve will not open when the system is actuated.

The AFW(ICS) flow control valve (FV-20527) is controlled by the ICS and is air operated. This valve would not be considered "safety related" because its power source (air) is not safety related and because the control is through the nonsafety-related ICS. Currently, SMUD depends upon manual (local) manipulation of the valve handwheel for flow control to prevent overfilling the OTSG and overcooling the reactor coolant system (RCS) if ICS control is not available or is not functioning properly. However, as discussed in Section 5.2, the manual operation of the AFW(ICS) flow control valves may be difficult.

Upon loss of instrument air, the AFW(ICS) flow control valve would go to the fully open position. However, if electric power to the plant instrument air system is lost, some time would be involved before the air receivers would depressurize sufficiently to cause the AFW (ICS) flow control valves to go to the open (loss-of-air) position. The current valve design does include a dc-powered solenoid-operated vent valve that can be operated remotely from the control room to immediately open the AFW (ICS) flow control valve. It is the Team's understanding that this feature was installed immediately after the TMI accident, but that later the operation of this vent was deleted from plant procedures and training and that SMUD intends to physically remove this vent in the near future.

It is also the Team's understanding that post-TMI requirement II.E.1.1 specifies that one train of AFW be operable for a postulated loss of main feedwater complicated by loss of offsite and onsite ac power sources. In such a case, the AFW would have to function on other power sources, such as steam and dc (i.e., battery) power. From the discussion above, it is clear that the

turbine-driven pump will operate only if the steam supply/isolation valve is actually in the open position. Also, the AFW(SFAS) flow control valve will remain closed without ac electric power. AFW flow then depends upon the AFW(ICS) flow control valve.

Under the postulated case, dc-powered devices may be considered. The ICS is powered by battery-operated inverters and therefore might be operable. Thus, AFW flow could be expected to occur if credit is allowed for the ICS or alternatively, through the operation of the dc-powered vent, assuming adequate procedures and training. However, the ICS is a nonsafety-related system, and credit is not normally given for such systems. Furthermore, control of the AFW(ICS) flow control valves would necessitate manual manipulation when instrument air is no longer available. Thus, manual operation of the AFW (ICS) valve would be required for long-term operation without ac power.

## 10 FINDINGS AND CONCLUSIONS

The incident at Rancho Seco on December 26, 1985, was significant because a single failure in the integrated control system (ICS), which is a nonsafety-related system, subjected the plant to an undesirable overcooling transient. During the transient, the RCS cooled down 180°F in 26 minutes, the pressurizer emptied, a bubble formed in the reactor vessel head, the plant entered the pressurized thermal shock region, the safety features actuation system (SFAS) actuated, and water overflowed from a steam generator into the main steam lines.

The fundamental causes for this transient were design weaknesses and vulnerabilities in the ICS and in the equipment controlled by that system. These weaknesses and vulnerabilities were not adequately compensated by other design features, plant procedures or operator training. These weaknesses and vulnerabilities were largely known to Sacramento Municipal Utility District (SMUD) and the NRC staff by virtue of a number of precursor events and through related analyses and studies. Yet, adequate plant modifications were not made so that this event would be improbable, or so that its course or consequences would be significantly altered. In summary, the information was available and known which could have prevented this overcooling transient; but in the absence of adequate plant modifications, the incident should have been expected.

### 10.1 Principal Findings and Conclusions

Based on the information available to the Team and its assessment, the following principal findings and conclusions are made relative to this event. There is no significance to the order in which they are presented.

1. The December 26, 1985 overcooling transient was initiated by the failure of a single module in the nonsafety-related ICS (i.e. the spurious tripping of the power supply module that interrupted all +/-24 Vdc power). The most probable cause of this failure was a design weakness that apparently made the circuit susceptible to erratic operation if "contact resistance" between the 24 Vdc bus and the power supply monitor were to develop, and the development of a high resistance connection (i.e. a bad crimp connection) in the wiring between the +24 Vdc bus and the power supply monitor which exposed the design weakness and caused the module to trip. (SMUD has agreed to further explore the cause of the failure of the power supply monitor by having an independent laboratory conduct additional analyses).
2. Upon loss of ICS dc power and the subsequent automatic repositioning of a number of valves in the plant, the design of the ICS also caused the loss of remote control of the affected valves from the control room which necessitates manual actions locally at the valves.
3. An AFW manual isolation valve could not be shut by the operators after the failure of the auxiliary feedwater (AFW) (ICS) flow control

valve. The failure of the AFW manual isolation valve was the result of a lack of any maintenance on this valve during the operational life of the plant. The lack of a maintenance program resulted in the valve being inadequately lubricated, which caused the valve to seize. It appears that the lack of a maintenance program could affect the operability of other manual valves at Rancho Seco.

4. Rancho Seco Emergency Operating Procedures (EOP) do not address the loss of ICS power. The lack of specific guidance seems to be a weakness in the plant-specific EOPs available to the operators on December 26, 1985. The Rancho Seco Anticipated Transient Operating Guidelines (ATOG) supplied by the B&W Owners Group include an explicit procedure for a loss of ICS power and the ATOG directs operators to that procedure. However, this procedure was not included in the Rancho Seco EOPs.
5. The EOPs at Rancho Seco direct the operators to trip the appropriate feed pumps to terminate flow if the feedwater flow cannot be isolated. This was not done during the December 26, 1985 incident. The operators were reluctant to stop the AFW pumps even when they had difficulty stopping flow to the once-through steam generators (OTSG) by valve operation. The operators had decided that they would stop the AFW pumps only if water started to flow into the main steam lines. However, the operators failed to adequately monitor OTSG water level and, as a result, water was introduced into the steam lines. Their reluctance appears to be the result of the substantial emphasis placed on the AFW system by NRC and others, and a lack of confidence in the reliability of the AFW pumps (i.e., fear that the pumps would not restart if stopped).
6. The operators had considerable difficulty reconciling the dichotomy between avoiding the pressurized thermal shock (PTS) region (e.g., reducing high pressure injection (HPI) flow) and regaining pressurizer level (e.g., increasing HPI flow in accordance with their EOPs). Their training and procedures were not adequate to resolve this conflict and to some extent tended to provide conflicting indications of the appropriate priorities.
7. The operators received neither classroom nor simulator training on the overall plant response to either the total loss of ICS dc power or the restoration of ICS dc power.
8. The operators who investigated the loss of ICS power did not adequately understand the ICS power system configuration. When 120 Vac power is still available from the 1C bus and the ICS dc power supplies de-energized, the most credible cause for the loss of ICS dc power was the opening of switches S1 and S2. However, the operators did not recognize this fact and, as a result, did not shut the switches until 26 minutes into the transient. The fact that several operators did not recognize that switches S1 and S2 were OFF suggests that their training on this crucial system was not adequate. In addition, although simplified drawings of the non-nuclear instrumentation (NNI) power supplies were posted on the NNI cabinets, comparable drawings for the ICS power supply had not been provided.

9. It does not appear that nonlicensed operators properly operated the AFW (ICS) flow control valves. An operator applied excessive force with a valve wrench to close an AFW (ICS) flow control valve. He did so because he had not accurately determined the position of the valve while attempting to shut it completely. As a result of his actions, the valve was damaged, reopened, and the manual (local) capability to operate the valve was lost. These consequences suggest training weaknesses in the acceptable use of valve wrenches, the proper methods for manually operating and overriding air-operated valves, and the use of available and backup indications to determine valve positions. These weaknesses suggest areas where hands-on training rather than walk-through or talk-through training may be necessary.
10. While the deficiencies in SMUD's radiological control and emergency preparedness programs during the December 26, 1985 incident did not jeopardize the public health and safety due to the relatively minor radiological consequences of this incident, they do indicate weaknesses in SMUD's program and the training of Rancho Seco personnel.
11. The NRC staff was led to believe that the emergency feedwater initiation and control (EFIC) system would be installed in 1984 in response to a number of NRC requirements, including TMI Action Item II.E.1.2. Apparently SMUD decided to install an alternate system in response to II.E.1.2. SMUD's intent to satisfy II.E.1.2 with this alternate design was not made clear to the NRC staff, was not approved by the staff, and may not have complied with the requirements of II.E.1.2. As a result, the EFIC system, some features of which would have reduced the severity of the December 26, 1985 incident, has not yet been installed at Rancho Seco.
12. Although the RCS temperature dropped 180°F in 26 minutes, it would have had to rapidly drop another 215°F (i.e., to an RCS temperature of about 170°F), while pressure was maintained at approximately 1400 psig, in order to seriously threaten reactor vessel integrity.
13. The December 26, 1985 overcooling incident does not appear to have seriously threatened the integrity of the Rancho Seco reactor vessel. However, the plant has had a number of overcooling incidents in its 12-year operating history. Each time this occurs the potential exists for additional operator errors and equipment failures that might exacerbate the event and seriously threaten reactor integrity. Thus, the significance of this incident lies in the fact that under alternate scenarios more serious consequences could occur.
14. It is not clear that the overcooling transient was within the Final Safety Analysis Report (FSAR) analysis of the Rancho Seco plant. Although PTS has been addressed generically, the FSAR accident analysis for Rancho Seco does not address this issue. The most comparable analysis in the FSAR is for the cooldown due to a main steam line break. However, this analysis includes only 100 seconds of the transient. In addition, the Rancho Seco FSAR analysis of main steam line breaks appears to be flawed and nonconservative in that it assumes that the nonsafety-related ICS operates successfully to mitigate the consequences of the accident.



15. There were a number of precursors to the December 26, 1985 incident at Rancho Seco. These precursors indicate that improvements in the reliability of the ICS and procedures to efficiently mitigate a loss of ICS power have not been developed or implemented at Rancho Seco despite numerous efforts on the part of the NRC staff to improve the reliability of the ICS and to ensure that the necessary procedures to efficiently mitigate such an event would be available to the operators. While the staff had raised these issues on a number of occasions over the past 6 to 8 years, SMUD personnel had not implemented the actions, and the NRC staff had not taken effective action to ensure that the improvements in reliability and the procedures were developed and implemented at Rancho Seco. The specific findings associated with these precursors include:
- a. Although the ICS power supply is similar to the NNI power supply, particularly with respect to the role of the power supply monitor, SMUD's principal emphasis following the lightbulb incident in March 1978 was on the NNI rather than on the ICS. This emphasis seems to have biased SMUD's subsequent reviews of issues associated with the NNI and ICS.
  - b. The loss of ICS power transient at Rancho Seco on January 5, 1979 was similar to the December 26, 1985 incident. However, it was not as severe as the "lightbulb incident" and did not receive the same level of attention. As a result, changes in the design of the ICS were not made and procedures for loss of ICS were not developed.
  - c. In March 1979, B&W issued a report (BAW-1564) in which they analyzed the reliability of the ICS. Although the B&W analysis noted a number of changes that appeared to be warranted in the ICS, SMUD concluded that no changes were necessary. A subsequent analysis of the ICS by the Oak Ridge National Laboratory criticized the B&W analysis and noted that it was of limited scope and did not appear to meet the requirements of the original Order. The NRC staff concluded that no immediate changes were required at Rancho Seco as a result of the B&W analysis. The long-term issues associated with the B&W report were to be considered in Unresolved Safety Issue (USI) A-47, "Safety Implications of Control Systems."
  - d. As a result of the loss of power to NNI and ICS at Oconee in November 1979, NRC issued Bulletin 79-27 describing a number of actions to be carried out by licensees. Although the Bulletin raised significant concerns about the consequences of a loss of power to instrumentation and control systems, SMUD concluded that no additional design modifications were necessary and that event-oriented procedures to deal with such events were not necessary. It would appear that Bulletin 79-27 was initially intended to solicit detailed information from licensees that could form the basis for an in-depth review of the issues associated with control systems comparable to the review of safety-related systems conducted as part of an operating license review. Based on the initial scope of the review, the conclusion was reached that SMUD's response did not contain sufficient information

and did not adequately address the concerns in the Bulletin. After the progressive narrowing of the scope of the review, it was decided that the SMUD response was adequate, despite what appear to be a number of weaknesses in the SMUD response. Thus, the conclusion was finally reached that SMUD had provided reasonable assurance that they had addressed the concerns in Bulletin 79-27, and that the long-term implications of Bulletin 79-27 would be addressed as part of USI A-47.

- e. Following the February 1980 loss of NNI power at Crystal River, the NRC identified an issue about the failure mode of atmospheric dump valves (ADV) on loss of ICS power. SMUD's response to this issue did not include the other valves at Rancho Seco that repositioned on loss of ICS power (i.e., they confined it to the narrow issue associated with the ADVs). In addition, SMUD deferred this narrow issue to installation of the EFIC system, which to date has not been installed at Rancho Seco. The NRC found this response to be acceptable.
- f. Because of concerns about the transient response of B&W-designed reactors and the role of ICS as an initiator of such transients, NRC conducted an extensive study and made 22 recommendations in NUREG-0667. However, it does not appear that these recommendations were sent to SMUD for action or that the recommendations that are relevant to the December 26, 1985 incident were implemented at Rancho Seco.
- g. The March 19, 1984 partial loss of NNI power at Rancho Seco again demonstrated that the failure of nonsafety-related equipment at B&W-designed plants has the potential to cause plant transients and to challenge the operator's capability to mitigate the transient without overcooling and undercooling the primary system. Despite the fact that this event occurred nearly 2 years ago, the December 26, 1985 incident demonstrates that neither SMUD nor the NRC staff has implemented effective actions to resolve this situation. In questions asked by the staff and responses provided by the B&W Owner's Group following the March 1984 loss of NNI power at Rancho Seco, the Team again sees strong evidence of a narrow focus on the incidents initiated by inappropriate control system actions in response to false inputs from the NNI. The questions in general do not refer directly to the ICS. As a result, the full significance of the loss of power to the ICS was not addressed.
- h. While the scope of the analysis performed under USI A-47 is broad, it appears that to date the actual study includes only those events with the potential to produce consequences outside the design basis of the reference plant. Such events are rare so the study does not appear to address substantive issues of the frequent challenges to protection systems and frequent abnormal operating occurrences, such as those identified in BAW-1564, Bulletin 79-27, and NUREG-0667. In addition, the analysis does not consider the events that are significant at other than the reference plant. Differences in plant design that could cause an event to be significant at another plant are not adequately considered. Therefore, it appears that the analysis performed to date under USI A-47 does not address the long-term issues raised

in Bulletin 79-27, BAW-1564, or NUREG-0667 that are relevant to the December 26, 1985 incident. Thus, results of the resolution of USI A-47 are of quite limited applicability to B&W-designed plants beyond the reference plant that was studied. The results are not directly applicable to most other B&W-designed plants such as Rancho Seco because of the differences in the design of the ICS.

## 10.2 Other Findings and Conclusions

1. It appears that the transient initiator (i.e., the loss of ICS dc power) was not fully recognized by control room operators until 2 minutes after the power was lost. Although the "ICS and Fan Power Failure" alarm alerts operators about ICS power failures, it appears that its importance was somewhat obscured because it also acts as a trouble alarm for fan failure or for loss of one of the redundant ICS dc power supplies, neither of which requires immediate operator actions or initiates a transient.
2. The Annunciator Procedures Manual was not used by the operators following the "ICS or Fan Power Failure" alarm. Even if the Annunciator Procedures Manual had been used, it contained very limited guidance concerning the implications of this alarm and would have been of no value to the operators in recognizing or restoring the loss of ICS dc power.
3. The ICS performance upon restoration of power are still not fully understood, especially because performance may depend on the duration of the power interruption. However, when ICS dc power is restored, reactor operators regain remote control of plant equipment from the control room. (It is the Team's understanding that the B&W Owner's Group is planning to conduct an investigative program that will include this matter.)
4. Most of the indicators in the control room (both meters and recorders) are part of the NNI system; hence, they are generally independent of the ICS. However, there are exceptions that had not been recognized prior to the December 26, 1985 incident. For example, the main feedwater (MFW) flow recorders are affected by the ICS. During the December 26, 1985 incident, the recorder failed to a value near mid-scale when MFW flow was actually zero.
5. Because of a perceived sense of urgency, two nonlicensed operators made an emergency entry into the makeup pump room without respiratory protection or adequate protective clothing, neither of which was readily available. As a result, their clothing was contaminated and they were exposed to airborne radioactivity.
6. The operators did not remember a recent modification had been made to permit the TBVs and ADVs to be closed from the remote shutdown panel (outside the control room) independent of the availability of ICS power. This change was made to accommodate a fire in the control room. Although this modification had been incorporated in the control room fire procedures, SMUD did not review other procedures to determine the applicability of this modification.

7. Additional staffing above that required by plant Technical Specifications and other SMUD regulatory commitments allowed operators to perform certain tasks simultaneously. With staffing at the minimum required level, the actions performed would have had to be performed sequentially, would have taken longer, and could have exacerbated the overcooling transient.
8. Neither the operators nor the Shift Technical Advisor (STA) could identify an instance of when the STA provided engineering expertise during the incident. However, the operators found the STA valuable as an extra person on shift to help out during the incident.
9. It appeared to the Team that SMUD personnel found the process of troubleshooting in a highly controlled, systematic, and well-documented manner, as proposed by the Team, to be quite different from their usual maintenance practices. This difference contributed to the difficulty that the Team experienced in reviewing the troubleshooting program.
10. Throughout the Team's review of the December 26, 1985 incident, SMUD personnel had considerable difficulty providing information in the detail that the Team requested. Thus, SMUD personnel repeatedly summarized data, analyses, and plans without including the actual data and analyses. As a result, the Team had to request the detailed underlying data and analyses, which subsequently were provided. This iterative process delayed the Team's onsite investigation.
11. In June 1983, the B&W Owner's Group reported (BAW-1791) the results of an analysis which predicted an overcooling transient caused by a loss of ICS power<sub>2</sub> could occur at B&W-designed reactors with a high probability (about  $4 \times 10^{-2}$  per reactor year). If this probability were applicable to all eight B&W-designed operating reactors, such a transient could occur at some B&W-designed plant approximately every 3 years. Thus, it would appear that this analysis predicts that events comparable to the December 26, 1985 incident would occur approximately once every third year even if the EFIC system were installed at all B&W-designed plants. In addition, the report notes that one B&W-designed plant has a combination of components that cause the transient frequencies to be even higher. The Team deduced that the plant was Rancho Seco. Finally, the generic B&W PTS analysis (BAW-1791) is not directly applicable to Rancho Seco because it assumes that the EFIC system is installed.



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

DEC 31 1985

MEMORANDUM FOR: Chairman Palladino  
Commissioner Roberts  
Commissioner Asselstine  
Commissioner Bernthal  
Commissioner Zech

FROM: William J. Dircks  
Executive Director for Operations

SUBJECT: INVESTIGATION OF DECEMBER 26, 1985 EVENT  
AT RANCHO SECO WILL BE CONDUCTED BY AN  
INCIDENT INVESTIGATION TEAM (IIT)

At about 4:15 a.m. on December 26, 1985, Rancho Seco experienced a loss of the Integrated Control System (ICS). Subsequently, the reactor tripped on high pressure and a severe overcooling transient occurred. Other equipment failures and personnel errors occurred. A radioactive release within technical specifications also occurred. An adequate subcooling margin was maintained throughout the event and the plant is now in cold shutdown.

Because of the potential significance of the event, an NRC Augmented Inspection Team (AIT) was sent to the site on December 27 and started transcribed personnel interviews on December 28. The initial results of this investigatory effort has indicated that this event is complex and has potentially significant generic implications. Consequently, I have directed that the investigation be upgraded and that an Incident Investigation Team (IIT) be established. This IIT is to: (a) fact find as to what happened; (b) identify the probable cause as to why it happened; and (c) make appropriate findings and conclusions which would form the basis for any necessary follow-on actions. A specific focus of the team will be on the design and response of ICS, and operator performance and training as they related to the loss of ICS during the event.

The team will report directly to me and will be led by Mr. Frederick Hebdon, Chief, Program Technology Branch, AEOD. Other team members include: J. T. Beard, NRR; R. Eaton, NRR; H. Bailey, IE; and G. Edison, NRR. The team was selected on the basis of their knowledge and experience in the fields of reactor systems, reactor operations, human factors, and instrumentation and control systems.

The licensee has agreed to a request by Jack Martin, Regional Administrator, to preserve the equipment in an "as-found" state until the licensee and the NRC Team have had an opportunity to evaluate the event. The licensee has also agreed to maintain the plant in a shutdown condition until concurrence is received from the NRC to return to power.

The Commission

- 2 -

The IIT report will constitute the single NRC fact-finding investigation report. It is expected that the team report will be issued within 45 days from now.

(Signed) William J. Dircks

William J. Dircks  
Executive Director for Operations

cc: SECY  
OPE  
OGC  
ACRS  
OPA  
Regional Administrators

NRC FORM 138 12 84 NRCM 1102 3201, 3207		U.S. NUCLEAR REGULATORY COMMISSION		REPORT NUMBER (Assign by NRC and not by User)	
<b>BIBLIOGRAPHIC DATA SHEET</b>			NUREG-1195		
2. TITLE AND SUBTITLE Loss of Integrated Control System Power and Overcooling Transient at Rancho Seco on December 26, 1985			3. LEAVE BLANK		
5. AUTHOR(S)			4. DATE REPORT COMPLETED MONTH YEAR February 1986		
7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code) Incident Investigation Team Executive Director for Operations U.S. Nuclear Regulatory Commission Washington, D. C. 20555			6. DATE REPORT ISSUED MONTH YEAR February 1986		
10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code) Same as 7 above			8. PROJECT/TASK WORK UNIT NUMBER		
12. SUPPLEMENTARY NOTES			9. FUND NUMBER		
11. ABSTRACT (200 words or less) On December 26, 1985, Rancho Seco Nuclear Generating Station, located in Clay, California, about 25 miles southeast of Sacramento, experienced a loss of dc power within the integrated control system (ICS) while the plant was operating at 76 percent power. The plant is owned by the Sacramento Municipal Utility District (SMUD). Following the loss of ICS dc power, the reactor tripped on high reactor coolant system (RCS) pressure followed by a rapid overcooling transient and automatic initiation of the safety features actuation system on low RCS pressure. The overcooling transient continued until ICS dc power was restored 26 minutes after its loss. The fundamental causes for this transient were design weaknesses and vulnerabilities in the ICS and in the equipment controlled by that system. These weaknesses and vulnerabilities were not adequately compensated by other design features, plant procedures or operator training. These weaknesses and vulnerabilities were largely known to SMUD and the NRC staff by virtue of a number of precursor events and through related analyses and studies. Yet, adequate plant modifications were not made so that this event would be improbable, or so that its course or consequences would be altered significantly. The information was available and known which could have prevented this overcooling transient; but in the absence of adequate plant modifications, the incident should have been expected. The report includes findings and conclusions of the NRC Incident Investigation Team sent to Rancho Seco by the NRC Executive Director for Operations in conformance with NRC's recently established Incident Investigation Program.			13. TYPE OF REPORT Incident Investigation		
14. DOCUMENT ANALYSIS - KEYWORDS/DESCRIPTORS integrated control system Rancho Seco overcooling transient transient Incident Investigation Team			15. AVAILABILITY STATEMENT unlimited		
			16. SECURITY CLASSIFICATION This page		
			This page		
			17. NUMBER OF PAGES		
			18. PRICE		

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

OFFICIAL BUSINESS  
PENALTY FOR PRIVATE USE, \$300

SPECIAL FOURTH-CLASS RATE  
POSTAGE & FEES PAID  
USNR  
WASH. D.C.  
PERMIT NO. 627

120555078877 1 1A19A19B19C  
USNR  
ADM-DIV OF TIOC  
POLICY & PUB MGT BR-PDR NUREG  
W-501  
WASHINGTON 20555