SNUPPS
Standardized Nuclear Unit
Power Plant System

5 Choke Cherry Road
Rockville, Maryland 20850
(301) 869-8010

Nicholas A. Petrick
Executive Director

August 14, 1981

SLNRC 81-68 FILE 0290
SUBJ: ICSB Review

Mr. Harold R. Denton, Director
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Docket Nos. STN 50-482, STN 50-483, and STN 50-486

Dear Mr. Denton:

Technical review meetings with the NRC's Instrumentation and Control Systems Branch were held on April 28, May 18-20, June 16-17, and July 27, 1981. The items discussed in this series of meetings were classified as agenda items # 1 through # 68 and ICSB positions # 1 through # 10. Enclosure A to this letter provides the status of the 68 agenda items. A separate SNUPPS letter addresses the 10 ICSB positions.

Three of the agenda items require attention beyond that given in Enclosure A.

#25 In addition to the FSAR changes included with this letter, there was a question concerning the testing of the reset capability of specific safety functions following a safety injection. The testing of the slave relays (GO-GO, NO-GO) causes certain relays to be mechanically latched up in the initiating circuits. The relays are unlatched by energizing the unlatch coil of the relay. Although this is done from the Safeguards test cabinets, the reset (unlatching) may be accomplished from the Control Room periodically to reconfirm the integrity of the wiring and associated components.

#45 SNUPPS plans to make design changes to help insure against inadvertent boron dilution. These changes are expected to be the same as those employed by Comanche Peak. The Comanche Peak design was reviewed and approved by the NRC staff. Confirmatory FSAR changes will be provided after engineering of the changes is more complete. It should be noted that the Reactor Systems Branch also requested the above information in an August 12, 1981 meeting.

B001
s
1/1

#52 The interface criteria provided in Appendices B and C of WCAP-8584, Revision 1 have been met in the SNUPPS design.

Enclosure B to this letter is the response to ICSB agenda item # 50 for the balance-of-plant. Enclosure C to this letter is the response to ICSB agenda item # 68. Enclosure D to this letter is a group of FSAR changes that will be included in SNUPPS FSAR Revision 6.

Very truly yours,

Nicholas A. Petrick

RLS/mtk3b20

Enclosure: A: Status of ICSB Agenda Items
B: Response to item # 50 - BOP
C: Response to item # 68
D: FSAR Changes

cc: J. K. Bryan UE
D. F. Schnell UE
G. L. Koester KGE
D. T. McPhee KCPL
W. A. Hansen NRC/CAL
T. E. Vandel NRC/WC

ENCLOSURE A

ICSB AGENDA ITEM	STATUS
1	Complete
2	See response to Q420.4 (FSAR Rev. 5)
3	See response to Q420.4 (FSAR Rev. 5)
4	Complete
5	See SLNRC 81-49 and SLNRC 81-63
6	See response to ICSB position # 1; SLNRC 81-67
7	Complete
8	See FSAR Rev. 5 (p. 7.3-25)
9	See FSAR Rev. 5 (T 7.1-4, sheet 2)
10	See FSAR Rev. 5 (T 7.1-7, sheet 2)
11	See response to ICSB position # 2; SLNRC 81-67
12	FSAR change included with this letter
13	See FSAR Rev. 5, Section 18.2.17.2.2. This section will be revised to address low condenser vacuum trip. Expected submittal; 8/31/81.
14	FSAR change included with this letter
15	Resolved by ICSB position # 4
16	FSAR change included with this letter
17	SLNRC 81-54 provided the plans for a design change to resolve this item. Confirmatory FSAR changes will be provided after engineering of the change is more complete.
18	Complete
19	FSAR change included with this letter
20	See FSAR Rev. 5 (T 7.3-8)
21	See FSAR Rev. 5 (T 7.3-11)
22	Complete
23	Complete
24	See FSAR Rev. 5 (p. 7.3-35)
25	FSAR change included with this letter. Also see cover letter.
26	Complete
27	Complete
28	Complete
29	Complete
30	Complete
31	See FSAR Rev. 5, Section 18.2.6.2
32	Complete
33	Complete
34	Response to Reg. Guide 1.97, Rev. 2 will be submitted later. Expected submittal: 8/31/81
35	Complete
36	See FSAR Rev. 5 (T 7.5-2, sheet 2)
37	Complete
38	See response to ICSB position # 7
39	FSAR changes to be provided later. Expected submittal: 8/31/81.
40	See FSAR Rev. 5 (p. 7.6-7)

ENCLOSURE A

ICSB AGENDA ITEM	STATUS
41	See response to ICSB position # 8; SLNRC 81-67
42	See response to ICSB position # 8; SLNRC 81-67
43	FSAR change included with this letter
44	Complete
45	This item is addressed in the cover letter
46	FSAR change included with this letter
47	Complete
48	FSAR change included with this letter
49	See FSAR Rev. 5 (T 7.2-3, pp. 7.3-35, 36)
50	For the BOP, see enclosure B to this letter. For the NSSS, a separate proprietary submittal will be made.
51	This item will be addressed later. Expected submittal 8/31/81.
52	This item is addressed in the cover letter.
53	See response to ICSB position # 9; SLNRC 81-67
54	SLNRC 81-54 provided the plans for a design change to resolve this item. Confirmatory FSAR changes will be provided after engineering of the change is more complete.
55	Complete
56	Complete
57	Complete
58	Resolved by ICSB position # 10
59	See response to Q420.2 (FSAR Rev. 5)
60	This item will be addressed later. Expected submittal: 8/31/81
61	Complete
62	Complete
63	See response to ICSB position # 8; SLNRC 81-67
64	Complete
65	Complete
66	See response to ICSB position # 2; SLNRC 81-67
67	See SLNRC 81-63
68	See enclosure C to this letter

RLS/3b23

ENCLOSURE B

ISCB Agenda Item # 50 BOP Scope

Comment "a": Provide a reference for the methodology used. Discuss any differences between the reference methodology and the methodology to be used by the applicants.

Response: The nominal setpoints and toleraces for the actuation of the balance of plant engineered safety features will include margin to ensure proper operation despite the statistical uncertainties of parameter measurement and of instrument trip points.

The uncertainty limit estimates will be based upon the following components:

a) basic inaccuracy (unrepeatability, nonlinearity, hysteresis, etc., as appropriate)
b) drift (bistables and associated cabinet-mounted devices will be calibrated monthly, all other devices will be calibrated every 18 months)
c) normal environment effects (assuming calibration at the lower environmental limits and operation at the upper limits)
d) power supply fluctuation effects
e) DEB effects: effects of either:
    1) additional environmental changes beyond the limits addressed in "c", or
    2) one SSE

    --whichever would result in the greater uncertainty. It is not necessary to consider the simultaneous existence of seismic effects and a design basis accident.

These uncertainty components will be individually addressed for each device in each instrument loop to be evaluated. As a first--and most conservative--estimate of the net uncertainty, the magnitudes of the components will simply be added together. If, in consideration of the parameter range, the normal and limiting parameter values, and other pertinent information, the resultant maximum uncertainty limit is found to be overly conservative, the uncertainty components will be evaluated to determine which result from statistically independent and which from common-mode phenomena. These components resulting from independent phenomena will be combined as the square root of the sum of the squares, and the remaining components will be added to the result.

Calibration uncertainties will be taken into account later by the individual SNUPPS Utilities.

ENCLOSURE B

ISCB Agenda Item # 50 BOP Scope

Comment "b": Verify that the environmental error allowances are based on the highest value determined in qualification testing.

Response: The environmental error allowances ("DBE effects" as defined in the response to comment "a") for BOP instruments will be based upon one of the following, as appropriate:

i) target specifications for maximum DBE-induced calibration change, if these specifications were met in qualification testing
ii) actual worst case calibration shifts measured in qualification testing
iii) adequately documented analysis and prediction of maximum calibration shifts

Comment "c": List the protection channels where the Technical Specifications setpoint, with allowance for channel statistical error, falls within 5% of the instrument range limit or within 5% of the range between level measurement taps. For those cases specify the remaining margin to the end of the range.

Response: When the parameter measurement uncertainty evaluations have been completed for the appropriae BOP protection channels, the resultant setpoints will be investigated. Those protection channels having setpoints without a margin of at least 5% of span to each range limit will be listed and reported to the NRC. At this time, no BOP protection channel is expected to fall into that category.

Comment "d": Document the enviromnental error allowance that is used for each reactor trip and engineered safeguards setpoint.

Response: The environmental error allowances for BOP engineered safeguards setpoints will be documented in the parameter measurement uncertainty evaluations. See the response to item "a".

Comment "e": Identify any time limits on environmental qualification of instuments used for trip, post-accident monitoring or engineered safety features actuation. Where instruments are qualified for only a limited time specify the basis for the limited time.

Response: The qualified life (this life will include consideration of the time for which each device will be required to function following a DBE) of the safety-related BOP instrumentation will be specified in FSAR Table 3.11(B)04. It is noted that nearly all of the safety related BOP instrumentation is located in plant areas that are not subject to hostile envoirnments.

ENCLOSURE B

ISCB Agenda Item # 50 BOP Scope

Comment "f": Address the effect of test equipment accuracy or setpoint errors.

Response: Test equipment accuracy will be taken into account by the individual SNUPPS Utilities and appropriate adjustments will be made to safety-related BOP instrument setpoints.

ENCLOSURE C

ISCB Agenda Item # 68

No credit is taken for shunt coil circuts of the reactor trip breakers. They are used only for additional assurance when the breakers are tripped with the manual trip switches at the control board. Each breaker is automatically tripped by de-energizing the undervoltage coil through the solid state protection system (SSPS). Independent dc power for two series-connected breakers is provided from the vital ac buses. The breakers and associated undervoltage circuits are Class 1E and meet all applicable criteria including on-line testability. Undervoltage coils are continuity tested using the semi-automatic test features of the SSPS as well as a functional (actual opening) test through the SSPS in accordance with surveillance test requirements of the plant Technical Specifications. In addition, the shunt and undervoltage power circuits are independent, and acceptable safety evaluations have taken no credit for existence of a shunt trip of the breakers.

RLS/3b26

the reactor if the power level is above P-7. The coincidence logic and interlocks are given in Table 7.2-1.

e. Steam generator low-low water level trip

The specific trip function generated is low-low steam generator water level trip.

This trip protects the reactor from loss of heat sink. This trip is actuated on two out of four low-low water level signals occurring in any steam generator.

The logic is shown on Figure 7.2-1 (Sheet 7).

f. Reactor trip on a turbine trip (anticipatory)

The reactor trip on a turbine trip is actuated by two-out-of-three logic from emergency trip fluid pressure signals or by all closed signals from the turbine steam stop valves. A turbine trip causes a direct reactor trip above P-9. The reactor trip on turbine trip provides additional protection and conservatism beyond that required for the health and safety of the public. This trip is included as part of good engineering practice and prudent design.

The turbine provides anticipatory trips to the reactor protection system from contacts which change position when the turbine stop valves close or when the turbine emergency trip fluid pressure goes below its setpoint.

Components specified for use as sensors for input signals to the reactor protection system for "emergency trip oil pressure low" and "turbine stop valves close" will conform to the requirements of IEEE 279-1971 and be environmentally qualified. However, seismic criteria are not included in qualification regarding mounting and location for that portion of the trip system located within nonseismic Category I structures.

Evaluations indicate that the functional performance of the protection system would not be degraded by credible electrical faults such as opens and shorts in the circuits associated with reactor trip or the generation of the P-7 interlock. The contacts of redundant sensors on the steam stop valves and the trip fluid pressure system are connected through the grounded side of the ac supply circuits in the solid state protection system. A ground fault would, therefore, produce no fault current. Loss of signal caused by open circuits would produce either a partial or full

ICSB
ITEM 12

reactor trip. Faults on the first stage turbine pressure circuits would result in upscale, conservative output for open circuits and a sustained current, limited by circuit resistance, for short circuits. Multiple failures imposed on these redundant circuits could potentially disable the P-13 interlock. In this event, the nuclear instrumentation power range signals would provide the P-7 safety interlock. Refer to functional diagram, Sheet 4 of Figure 7.2-1.

Evaluations provided in Section 7.6.1 for the trip fluid pressure transmitter loops indicate that credible electrical faults would not degrade the functional performance of the safety-related BOP instrumentation.

In addition, the following measures will be taken to ensure the integrity of the cabling to the reactor protection system (RPS):

1. Inputs from the turbine steam stop valves will originate from four separate limit switches (one per valve), each of which is dedicated to providing an input to one channel of the RPS. Cables carrying these signals will be routed in individual conduits. The four circuits will be separated from one another, from non-Class IE circuits, and identified according to the criteria imposed on Class IE circuits from their source up to their terminations with the RPS cabinets.

2. Inputs from the emergency trip oil pressure instrumentation will be routed in a similar manner as are the turbine stop valve inputs.

The logic for this trip is shown on Figure 7.2-1 (Sheet 16).

ICSB
I.F-M 12

g. Safety injection signal actuation trip

A reactor trip occurs when the safety injection system is actuated. The means of actuating the safety injection system are described in Section 7.3. This trip protects the core following a loss of reactor coolant or a steam line rupture. S

Figure 7.2-1 (Sheet 8) shows the logic for this trip.

h. Manual trip

The manual trip consists of two switches with two outputs on each switch. One output is used to actuate the train A reactor trip breaker; the other output actuates the train B reactor trip breaker. Operating a manual trip switch removes the voltage from the undervoltage trip coil and energizes the shunt trip coil of each breaker.

There are no interlocks which can block this trip. Figure 7.2-1 (Sheet 3) shows the manual trip logic. The design conforms to Regulatory Guide 1.62, as shown in Figure 7.2-3.

7.2.1.1.3 Reactor Trip System Interlocks

See Table 7.2-2 for the list of projection system interlocks.

a. Power escalation permissives

The overpower protection provided by the out-of-core nuclear instrumentation consists of three discrete, but overlapping, ranges. Continuation of startup operation or power increase requires a permissive

ICSB
ITEM 12

7.6 ALL OTHER INSTRUMENTATION SYSTEMS REQUIRED FOR SAFETY

7.6.1 INSTRUMENTATION AND CONTROL POWER SUPPLY SYSTEM

The instrumentation and control power supply system is described in Section 8.3.1.1.5.

Safety-related BOP transmitters not powered directly from the system described in 8.3.1.1.5 are powered by input buffers in the BOP analog equipment cabinets.

Each BOP electronic analog input buffer is able to withstand an open circuit, a short circuit, or a single or multiple-point ground on the field wiring, without affecting any other instrument loop in any separation group.

An open circuit would interrupt the field current and drive the buffer output offscale "low." The field bus power supply voltage is not high enough to cause any damage if it were suddenly unloaded. There would be no consequential damage to the electronics.

A short circuit would apply the full field bus voltage across on-board current-limiting resistors designed and provided to limit such current to a safe value. The buffer output would be driven to the high limit with no consequential damage to the electronics.

A single ground on an input buffer field line would connect one side of the field bus power supply to system ground through an on-board, current-limiting resistor designed and provided to limit the resultant current to a safe value. The buffer output would take on some arbitrary value, with no consequential damage to the electronics.

A ground on both field lines of an input buffer would result in a condition similar to an input line short circuit. The buffer output would be driven to the high limit, but there would be no consequential damage to the electronics.

7.6.2 RESIDUAL HEAT REMOVAL SYSTEM ISOLATION VALVES

7.6.2.1 Description

The residual heat removal system (RHRS) isolation valves are normally closed and are opened only for residual heat removal system operation after system pressure is reduced to approximately 425 psig and system temperature has been reduced to approximately 350 F.

ICSB
ITEM 2

There are two motor-operated valves in series in each of the two residual heat removal pump suction lines from the reactor coolant system (RCS) hot legs. The two valves nearest the RCS (valves 8702A and 8702B) are designated as the inner isolation valves, while the two valves nearest the residual heat removal pumps (valves 8701A and 8701B) are designated as the outer isolation valves. The interlock features provided for the outer isolation valves, shown on Figure 7.6-1 (Sheet 1), are identical to those provided for the inner isolation valves, shown on Figure 7.6-1 (Sheet 2), except that equipment diversity is employed by virtue of the fact that PT 405 is of a different manufacture than PT 403.

Each valve is interlocked so that it cannot be opened unless the RCS pressure is below a preset pressure. This interlock prevents the valve from being opened when the RCS pressure plus the residual heat removal pump pressure is above the RHRS design pressure. A second pressure interlock is provided to close the valve automatically if the RCS pressure subsequently increases to above a preset value.

In addition, the valves cannot be opened unless the isolation valves in the following lines are closed:

a. Recirculation line from the residual heat exchanger outlet to the suction of the high head safety injection pumps.

b. RHR pump suction line from the refueling water storage tank.

c. RHR pump suction line from the containment sump.

ICSB
ITEM 4

DISCUSSION:

The recommendations of this regulatory guide are met. Refer to Section 3.3.

REGULATORY GUIDE 1.118 REVISION 2 DATED 6/78

Periodic Testing of Electric Power and Protection Systems

DISCUSSION:

For the systems not provided with the NSSS, the recommendations of this regulatory guide are met as described in Table 7.1-7.

For systems provided with the NSSS, Westinghouse follows the recommendations of the regulatory guide with the following exceptions:

Westinghouse defines "Protective Action Systems" to mean the electric instrumentation and controls portions of those protection systems and equipment actuated and controlled by the protection system.

Equipment performing control functions, but actuated from protection system sensors, is not part of the safety system and will not be tested for time response.

Status, annunciating, display, and monitoring functions, except those related to the post-accident monitoring system (PAMS), are considered by Westinghouse to be control functions. Reasonability checks, i.e., comparison between or among similar such display functions, will be made.

Response time testing for control functions operated from system sensors will not be performed. Moreover, NIS detectors will not be tested for time response, since their worst case response time is not a significant fraction of the total overall system response (i.e., less than 5 percent). Despite the fact that this exemption is no longer permitted by IEEE-338 (1977 version), Westinghouse believes that it is valid.

Refer to Section 7.1.2.6.2 for additional discussions on response time testing of protection sensors.

REGULATORY GUIDE 1.119 REVISION NA DATED NA

Surveillance Programs for New Fuel Assembly Designs

ICSB
ITEM 14

g. Reactor coolant pump seal water return valves (close)

Seal water return line isolation valves are routinely tested during refueling outages. Closure of these valves during operation would cause the seal water system relief valve to lift, with the possibility of valve chatter. Valve chatter could damage this relief valve. Testing of these valves at power could cause equipment damage. Therefore, these valves will be tested during scheduled refueling outages. As above, additional containment penetrations and containment isolation valves introduce additional unnecessary potential pathways for radioactive release following a postulated accident. Thus, the guidelines of Regulatory Position D.4 of Regulatory Guide 1.22 are met.

7.1.2.6 Conformance to IEEE Standards

7.1.2.6.1 Conformance to IEEE Standard 379-1972

The principles described in IEEE Standard 379-1972 were used in the design of the Westinghouse protection system. The system complies with the intent of this standard and the additional guidance of Regulatory Guide 1.53, although the formal analyses have not been documented exactly as outlined. Westinghouse has gone beyond the required analyses and has performed a fault tree analysis (Ref. 1).

The referenced report provides details of the analyses of the protection systems previously made to show conformance with the single failure criterion set forth in Section 4.2 of IEEE Standard 279-1971. The interpretation of the single failure criterion provided by IEEE Standard 379-1972 does not indicate substantial differences with the Westinghouse interpretation of the criterion, except in the methods used to confirm design reliability. The RTS and ESFAS are each redundant safety systems. The required periodic testing of these systems will disclose any failures or loss of redundancy which could have occurred in the interval between tests, thus ensuring the availability of these systems.

7.1.2.6.2 Conformance to IEEE Standard 338-1971

The periodic testing of the RTS and ESFAS conforms to the requirements of IEEE Standard 338-1971 with the following comments:

a. The surveillance requirements of Chapter 16.0 for the protection system ensure that the system functional operability is maintained comparable to the original design standards. Periodic tests at the established intervals demonstrate this capability for the system.

ICSB
ITEM 14

For sensors, the method used will function on the principle that, in the protection system, sensors are sensitive to process noise created by natural perturbations in variables, including temperature, pressure, and flow. Nuclear instrumentation detectors are excluded since delays attributable to them are negligible in the overall channel response time required for safety.

The noise method testing system is designed to measure sensor response time and/or assess degradation by measurement of the sensor's efficiency to detect high-frequency noise. Data collected from each sensor is conditioned, amplified, digitized, and analyzed by an on-board microcomputer. Two analyses are performed. One compares the obtained frequency signature with a baseline signature for checking degradation, the other compares the cutoff frequency of the power density spectrum to estimate response time.

The sensor response time testing system is mobile and can collect and analyze data from four primary or secondary system detectors at the same time. RTDs, pressure transmitters, and DP cells can be tested with the reactor between 50- and 100-percent power.

The measurement of response time at the specified time intervals provides assurance that the protective and engineered safety feature action function associated with each channel is completed within the time limit assumed in the accident analyses.

b. The reliability goals specified in Section 4.2 of IEEE Standard 338-1971 are consistent with the test frequency in Chapter 16.0.

c. The periodic time interval discussed in Section 4.3 of IEEE Standard 338-1971, and specified in Chapter 16.0, is selected to ensure that equipment associated with protection functions has not drifted beyond its minimum performance requirements. The adequacy of the interval will be verified by results of testing or the interval will be reevaluated on the basis of actual experience.

d. The test interval discussed in Section 5.2 of IEEE Standard 338-1971 is developed primarily on past operating experience and modified, if necessary, to ensure that system and subsystem protection is reliably provided. Analytic methods for determining reliability are not used to determine test interval.

IC SB
IEM 14

7.1.3 REFERENCES

1. Gangloff, W.C. and Loftus, W.D., "An Evaluation of Solid State Logic Reactor Protection in Anticipated Transients," WCAP-7706-L (Proprietary) and WCAP-7706 (Non-Proprietary), July, 1971.

2. Marasco, F.W. and Siroky, R.M., "Westinghouse 7300 Series Process Control System Noise Tests," WCAP-8892-A, June, 1977.

3. Letter dated April 20, 1977, R.L. Tedesco (NRC) to C. Eicheldinger (Westinghouse).

ICSB
ITEM 16

Plant systems and equipment which are available to mitigate the effects of the accident are discussed in Section 15.0.8 and listed in Table 15.0-6. No single active failure in any of these systems or equipment will adversely affect the consequences of the accident.

Results

Figures 15.5-1 through 15.5-3 show the transient response to inadvertent operation of ECCS during power operation. Neutron flux starts decreasing immediately due to boron injection, but steam flow does not decrease until later in the transient when the turbine throttle valve goes wide open. The mismatch between load and nuclear power causes T_{avg}, pressurizer water level and pressurizer pressure to drop. When the low pressure trip set point is reached, the reactor trips and control rods start moving into the core. Departure from nucleate boiling ratio (DNBR) increases throughout the transient.

The calculated sequence of events is shown on Table 15.5-1. After reactor trip, pressure and temperature slowly rise since the turbine is tripped and the reactor is producing some power due to delayed neutron fissions and decay heat. Recovery from this accident is discussed in Section 15.5.1.1.

15.5.1.3 Conclusions

Results of the analysis show that spurious ECCS operation without immediate reactor trip presents no hazard to the integrity of the RCS.

If the reactor does not trip immediately, the low pressurizer pressure reactor trip will be actuated. This trips the turbine and prevents excess cooldown, thereby expediting recovery from the incident.

15.5.2 CHEMICAL AND VOLUME CONTROL SYSTEM MALFUNCTION THAT INCREASES REACTOR COOLANT INVENTORY

15.5.2.1 Identification of Causes and Accident Description

Increases in reactor coolant inventory caused by the chemical and volume control system may be postulated to result from operator error or a false electrical signal. Transients examined in this section are characterized by increasing pressurizer level, increasing pressurizer pressure, and constant boron concentration. The transients analyzed in this section are done to: demonstrate that there is adequate time for the operator to take corrective action to prevent

ICSB
ITEM 16

filling the pressurizer. An increase in reactor coolant inventory, which results from the addition of cold, unborated water to the RCS, is analyzed in Section 15.4.6, chemical and volume control system malfunction that results in a decrease in boron concentration in the reactor coolant. An increase in reactor coolant inventory which results from the injection of highly borated water into the RCS is analyzed in Section 15.5.1, inadvertent operation of the emergency core cooling system during power operation.

Transients postulated as a result of operator error or failure of the charging pump controller which increase primary side inventory will be automatically terminated by a high pressurizer level reactor trip before the pressurizer can be filled, thus these are not the worst cases.

The most limiting case would result if charging was in automatic control and the pressurizer level channel being used for charging control failed in a low direction. This would cause maximum charging flow to be delivered to the RCS and letdown flow would be isolated. The worst single failure for this event would be another pressurizer level channel failing in an as is condition or a low condition. This will defeat the reactor trip on two out of three high pressurizer level channels. To prevent filling the pressurizer the operator must be relied upon to terminate charging.

15.5.2.2 Analysis of Effects and Consequences

Method of Analysis

The charging malfunction is analyzed by employing the detailed digital computer program LOFTRAN (Ref. 1). The code simulates the neutron kinetics, RCS, pressurizer, pressurizer relief and safety valves, pressurizer spray, steam generator, steam generator safety valves, and the effect of the SIS. The program computes pertinent plant variables, including temperatures, pressures, and power level.

Four cases were analyzed;

a. Minimum reactivity feedback with automatic pressurizer spray

b. Minimum reactivity feedback without automatic pressurizer spray

c. Maximum reactivity feedback with automatic pressurizer spray

d. Maximum reactivity feedback without automatic pressurizer spray

ICSB
ITEM 16

The assumptions incorporated in the analyses were as follows;

a. Initial Operating Conditions

The initial reactor power, RCS temperature, and pressurizer level are assumed at their maximum values consistent with steady state full power operation, including allowance for calibration and instrument errors. Pressurizer pressure is assumed to be initially at its minimum value.

b. Reactivity Coefficients

1. Minimum Reactivity Feedback Case

A least negative moderator temperature coefficient and a least negative doppler-only power coefficient.

2. Maximum Reactivity Feedback Case

A conservatively large negative moderator temperature coefficient and a most negative doppler only power coefficient.

c. Reactor Control

The reactor was assumed to be in manual control. As shown in Figures 15.5-4 through 15.5-11, core power and average RCS temperature change very little, thus the effects of automatic rod control would be negligible.

d. Charging System

Maximum charging system flow based on RCS back pressure from one centrifugal charging pump is delivered to the RCS. The charging flow is assumed to have the same boron concentration as the RCS.

e. Reactor Trip

The transient is initiated by the pressurizer level channel which is used for control purposes failing low. As a worst single failure, another pressurizer level channel fails low, defeating the two out of three high pressurizer level trip.

RESULTS

Figures 15.5-4 through 15.5-11 show the transient response due to the charging system malfunction. In all the cases analyzed, core power and RCS average temperature remain relatively constant.

IE 53
ITEM 16

Cases where the pressurizer spray is inoperable show the pressurizer level increases at a relatively constant rate. This is because the pressurizer pressure initially rises very quickly to the pressure at which the relief valves open and remains there.

Cases where the pressurizer spray is operable show the pressurizer level increases with varying rates. Spray actuation tends to keep the pressurizer pressure lower for several minutes, which allows the charging pumps to deliver more flow. Eventually, pressurizer pressure does increase enough to open the relief valves.

Times at which the operator would receive alarms are listed in Table 15.5-1.

15.5.2.3 Conclusions

Results show none of the operating conditions during the transient approach core limits. Because the high pressurizer level trip has been defeated by failures, the transient must be terminated by the operator. The sequence of events presented in Table 15.5-1 show the operator has sufficient time to take corrective action.

IESB
ITEM:6

TABLE 15.5-1 (Sheet 1)

TIME SEQUENCE OF EVENTS FOR INCIDENTS WHICH RESULT IN AN INCREASE IN REACTOR COOLANT INVENTORY

Accident	Event	Time (sec)
Inadvertent actuation of the ECCS during power operation	Spurious SIS generated; two centrifugal charging pumps begin injecting borated water	0.0
	Turbine throttle valve wide open; load begins to drop with steam pressure	21.5
	Low pressurizer pressure reactor trip setpoint reached	30.5
	Control rod motion begins	32.5
Chemical and volume control system malfunction, minimum reactivity feedback, without pressurizer spray	Two pressurizer level channels fail low	0.0
	Maximum charging flow from one centrifugal charging pump is begun	
	Letdown is isolated	
	Lo-lo-pressurizer level alarm	
	HI pressurizer pressure alarm	105
	Pressurizer relief valve setpoint reached	130
	HI pressurizer level alarm from the one working level channel	1,223
	Pressurizer fills	1,532

IE SB
ITEM 16

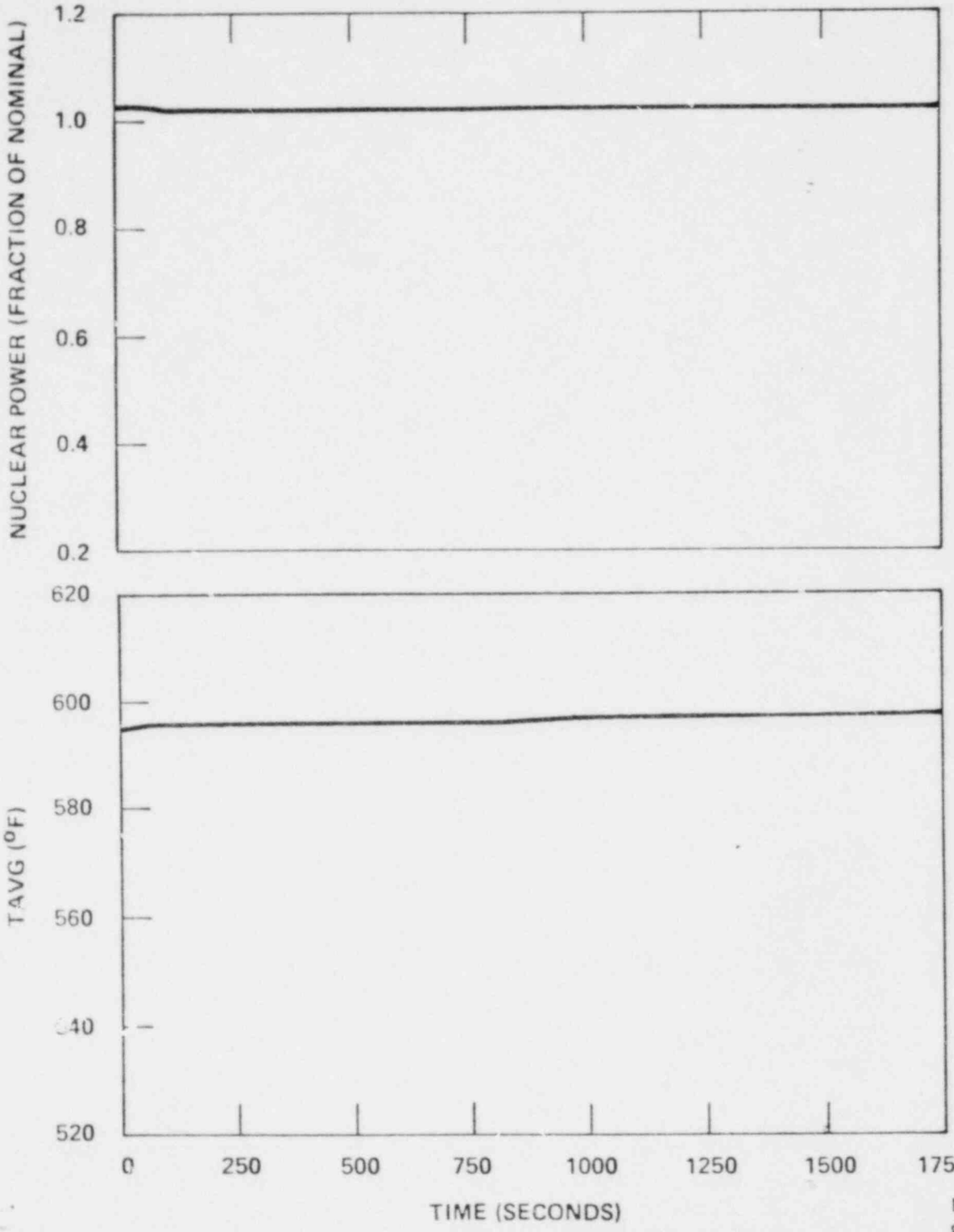
TABLE 15.5-1 (Sheet 2)

Chemical and volume control system malfunction, minimum reactivity feedback, with pressurizer spray	Two pressurizer level channels fail low	0.0
	Maximum charging flow from one centrifugal charging pump is begun	
	Letdown is isolated	
	Lo-lo pressurizer level alarm	
	Pressurizer spray actuated	55
	Hi pressurizer level alarm from the one working channel	739
	Hi pressurizer pressure alarm	958
	Pressurizer relief valve setpoint reached	1,057
	Pressurizer fills	1,473
Chemical and volume control system malfunction, maximum reactivity feedback, without pressurizer	Two pressurizer level channels fail low	0.0
	Maximum charging flow from one centrifugal charging pump is begun	
	Letdown is isolated	
	Lo-lo pressurizer level alarm	
	Hi pressurizer pressure alarm	65
	Pressurizer relief valve setpoint reached	78
	Hi pressurizer level alarm from the one working level channel	951
	Pressurizer fills	1,346

ICSB
ITEM 16

TABLE 15.5-1 (Sheet 3)

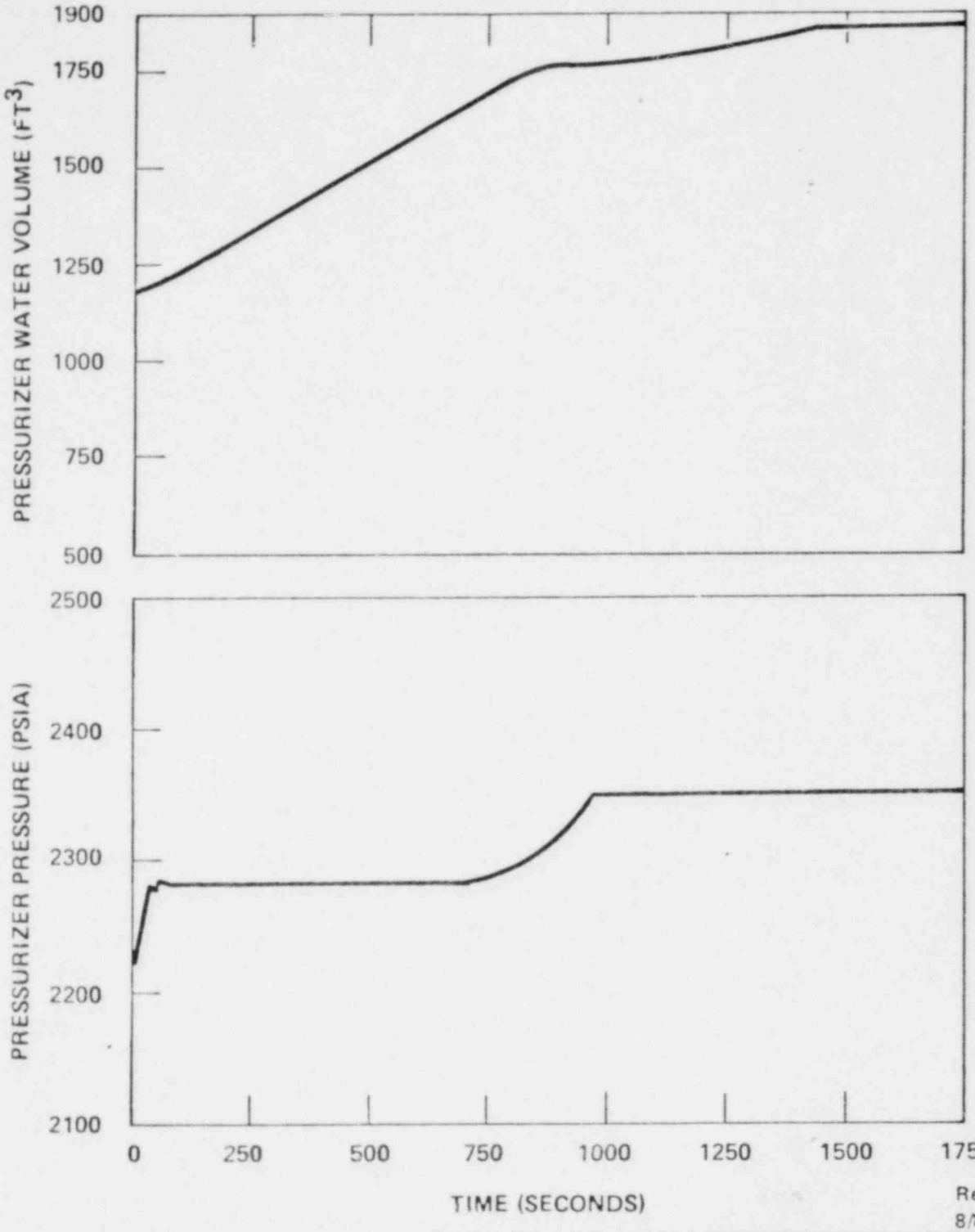
Chemical and volume control system malfunction, maximum reactivity feedback, without pressurizer spray	Two pressurizer level channels fail low	0.0
	Maximum charging flow from one centrifugal charging pump is begun	
	Letdown is isolated	
	Lo-lo pressurizer lev alarm	
	Pressurizer spray actuated	40
	Hi pressurizer level alarm from the one working level channel	693
	Hi pressurizer pressure alarm	906
	Pressurizer relief valve setpoint reached	1,013
	Pressurizer fills	1,429



Rev. 6
8/81

SNUPPS

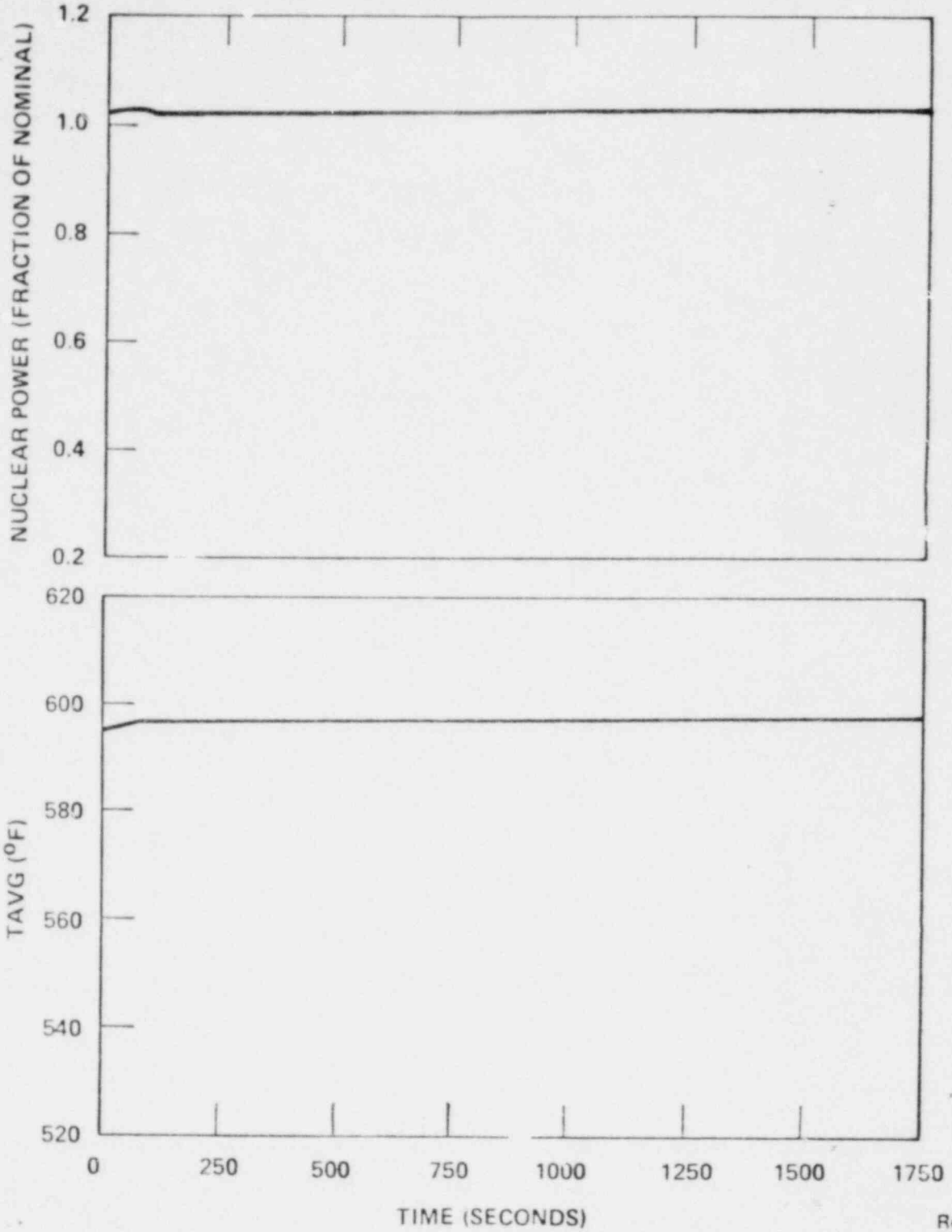
FIGURE 15.5-11
CHEMICAL AND VOLUME CONTROL
SYSTEM MALFUNCTION MAXIMUM
REACTIVITY FEEDBACK, WITH
PRESSURIZER SPRAY



Rev. 8/81

SNUPPS

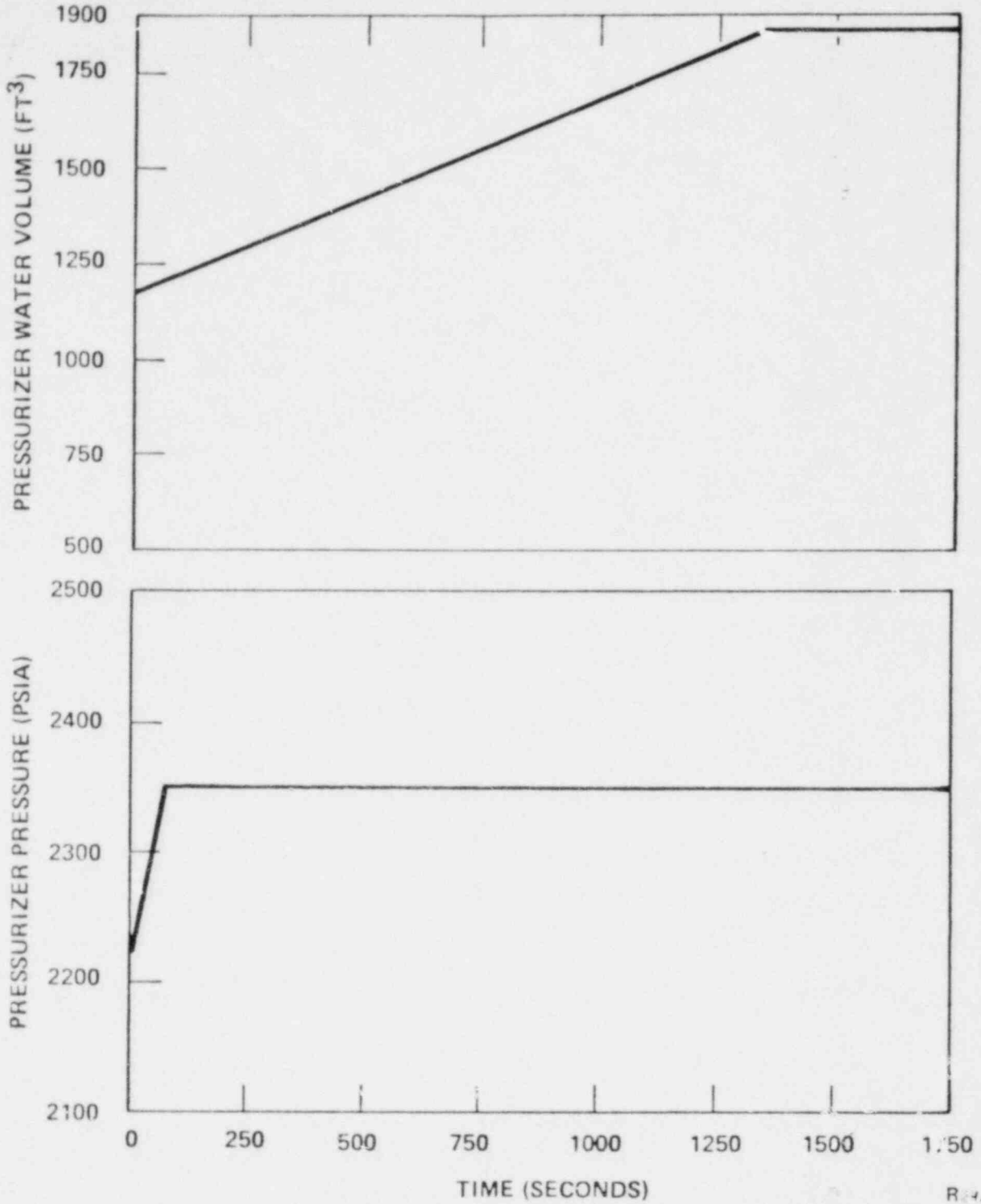
FIGURE 15.5-10
CHEMICAL AND VOLUME CONTROL SYSTEM MALFUNCTION MAXIMUM REACTIVITY FEDBACK, WITH PRESSURIZER SPRAY



Rev. 6
8/81

SNUPPS

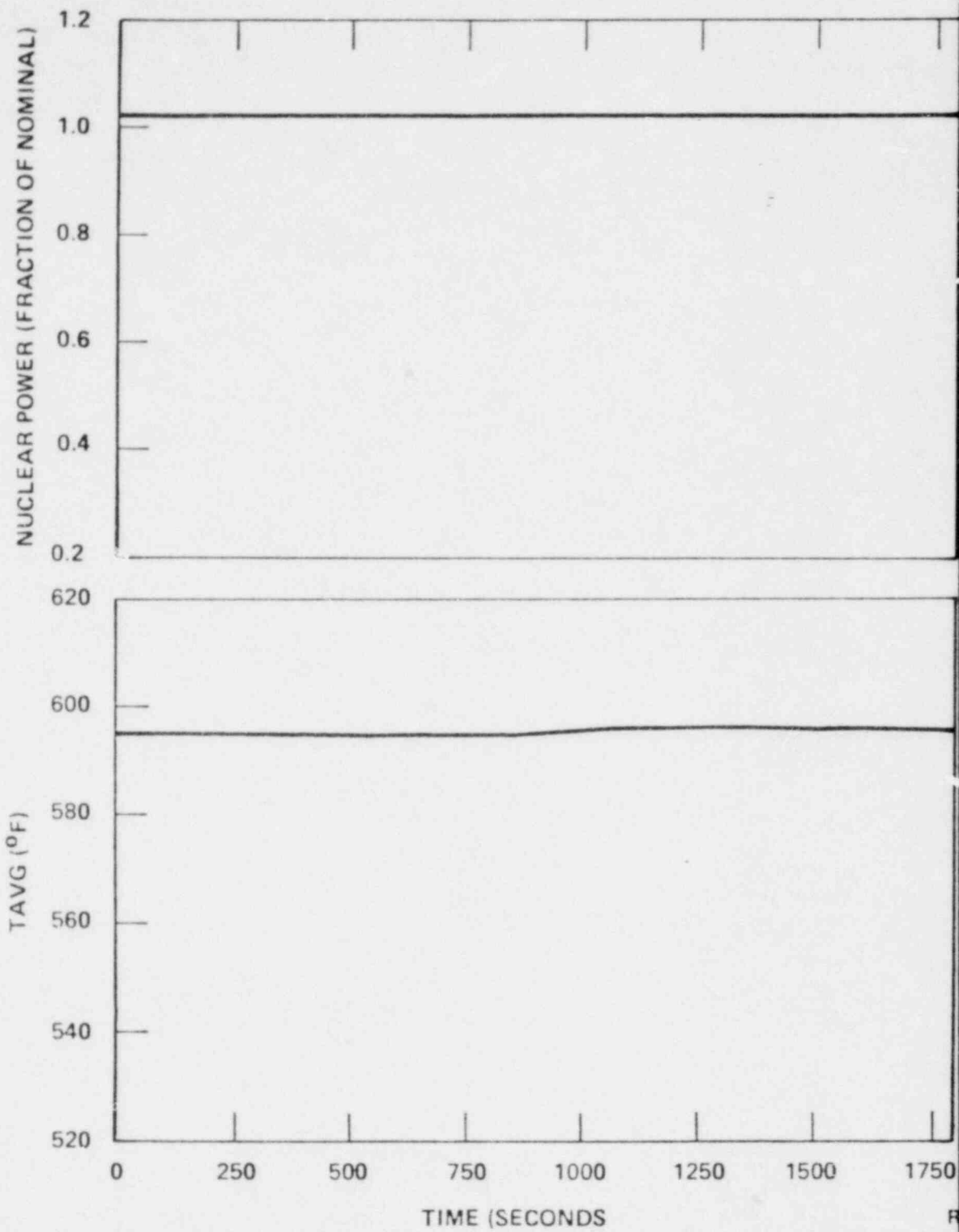
FIGURE 15.5-9
CHEMICAL AND VOLUME CONTROL SYSTEM MALFUNCTION MAXIMUM REACTIVITY FEEDBACK, WITHOUT PRESSURIZER SPRAY



Rev. 6
8/81

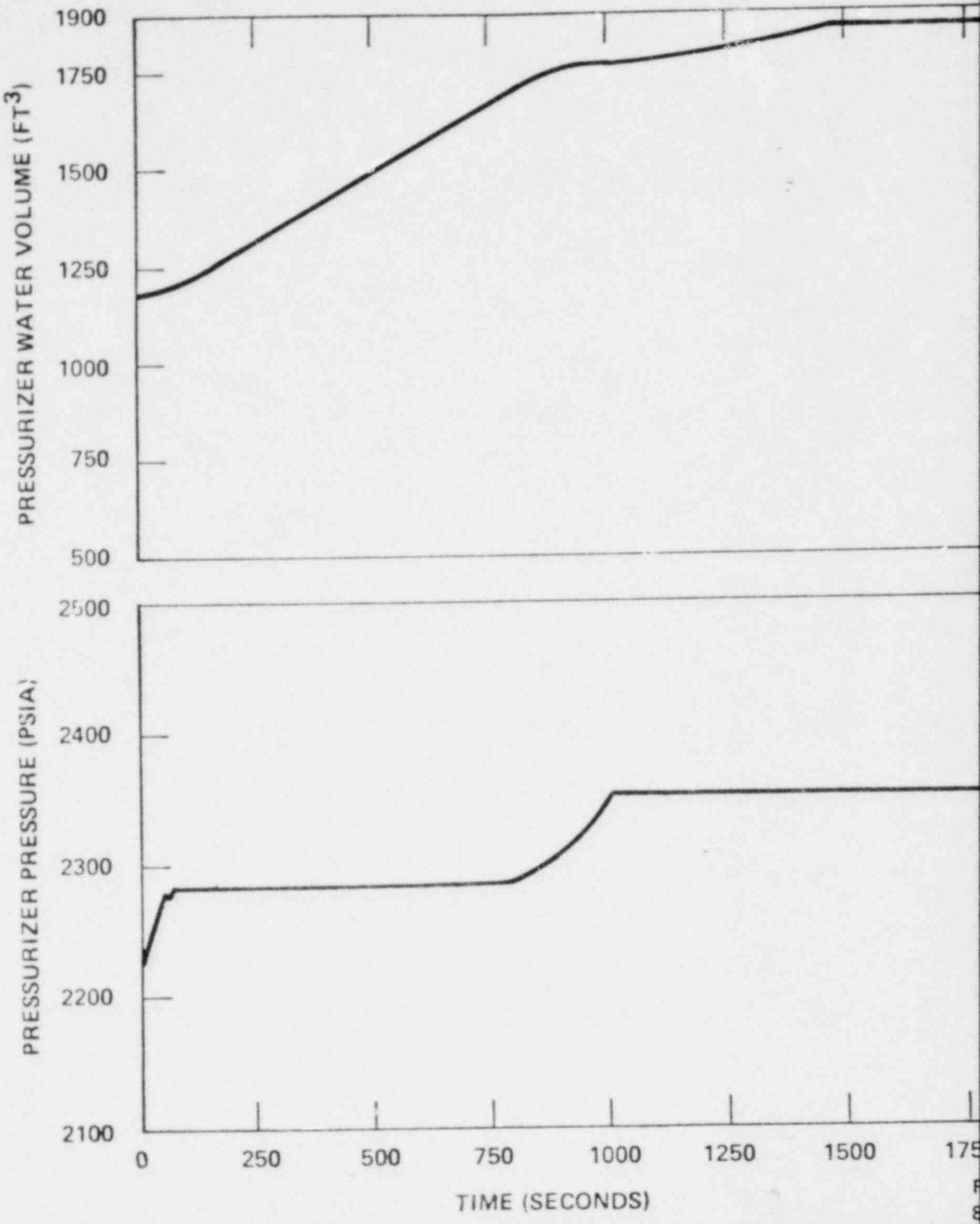
SNUPPS

FIGURE 15.5-8
CHEMICAL AND VOLUME CONTROL SYSTEM MALFUNCTION MAXIMUM REACTIVITY FEEDBACK, WITHOUT PRESSURIZER SPRAY



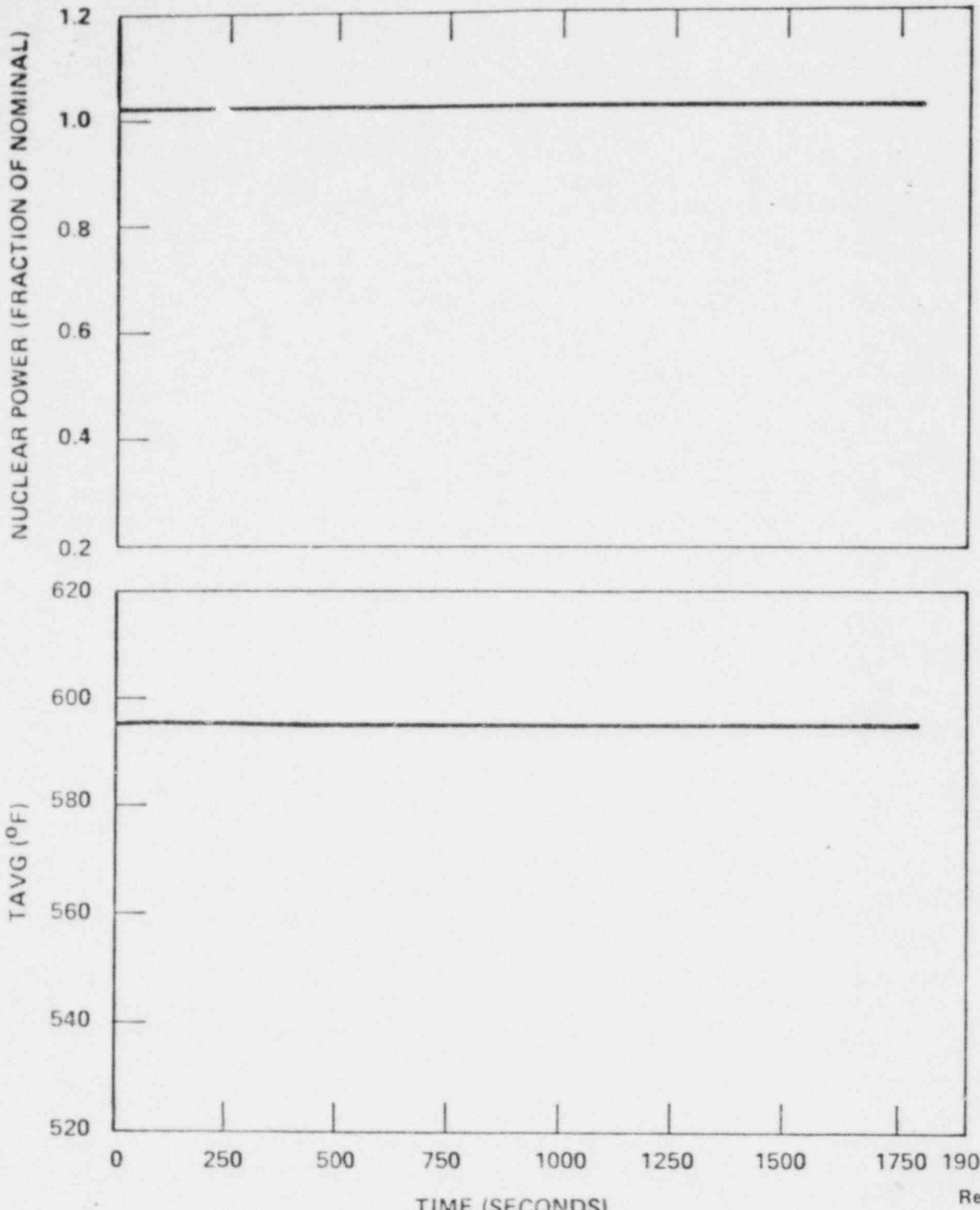
SNUPPS

FIGURE 15.5-7
CHEMICAL AND VOLUME CONTROL SYSTEM MALFUNCTION MINIMUM REACTIVITY FEEDBACK, WITH PRESSURIZER SPRAY



SNUPPS

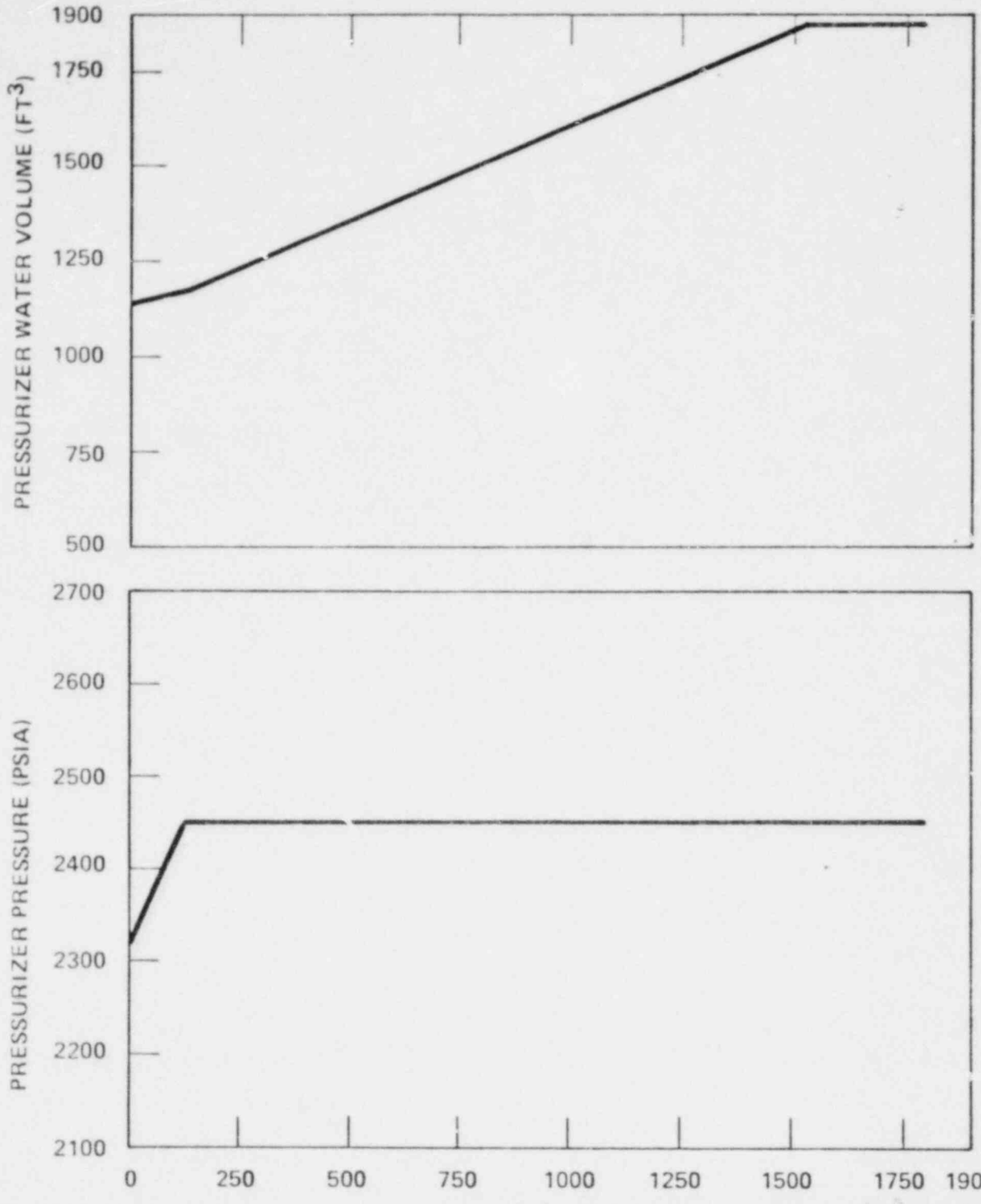
FIGURE 15.5-6
CHEMICAL AND VOLUME CONTROL SYSTEM MALFUNCTION MINIMUM REACTIVITY FEEDBACK, WITH PRESSURIZER SPRAY



Rev. 6
8/81

SNUPPS

FIGURE 15.5-5
CHEMICAL AND VOLUME CONTROL SYSTEM MALFUNCTION MINIMUM REACTIVITY FEEDBACK, WITHOUT PRESSURIZER SPRAY



Rev. 6
8/81

SNUPPS

FIGURE 15.5-4
CHEMICAL AND VOLUME CONTROL SYSTEM MALFUNCTION MINIMUM REACTIVITY FEEDBACK, WITHOUT PRESSURIZER SPRAY

IE SB
ITEM 19

7.3.2 CONTAINMENT PURGE ISOLATION SYSTEM

7.3.2.1 Description

The containment purge isolation system detects any abnormal amount of radioactivity in the containment atmosphere or in the containment purge effluent, and initiates appropriate action to ensure that any release of radioactivity to the environs is controlled. The containment purge systems are also isolated by CIS.

7.3.2.1.1 System Description

a. Initiating circuits

Redundant and independent gaseous radiation monitors measure the radioactivity levels of the containment atmosphere and of the containment purge effluent. These monitors provide analog radioactivity signals to bistable units in the ESF actuation system. The bistables generate redundant trip signals, and transmit them to the automatic actuation logic. Since the dampers also close on CIS, the initiating logic for CIS shown in Figure 7.2-1 (Sheet 8) is also applicable.

b. Logic

A logic diagram for the ESF actuation system is provided as Figure 7.3-1. This diagram shows only the actuation systems; it does not detail the bypass, bypass interlock, or test provisions. The logic for the containment purge isolation actuation subsystem is included in this figure.

The ESFAS hardware consists of solid-state bistables and logic elements, with electromechanical relays as the final output devices. The output relays are all energize-to-actuate, with contact operation as required for each actuated device.

The ESFAS is divided into three input-logic-output channels. These channels all meet the independence and separation criteria, as described elsewhere in this chapter. The logic channels are uniquely associated with the output channels. The input signals from all three input channels are isolated as necessary, and the isolated signals are transmitted to the logic channels as shown in Figure 7.3-1.

Interconnection of differing separation groups within the BOP ESFAS is by means of digital signal isolation modules. Analog signal isolation modules are included to provide isolated analog signals to the BOP computer. Adequate physical separation or barriers are provided

LCSE
LTCM19

between differing separation groups, and wiring is routed in separated wireways, where appropriate. The wiring is color-coded with regard to separation group.

The digital signal isolation modules utilize optical isolators with appropriate signal and power conditioning circuits. The output circuits are powered by the devices receiving signals from the isolation modules, so no power isolation is required. There are no connections between the input and output circuits, except for the optical coupling in the isolation devices.

The analog signal isolation modules utilize transformers as the isolation devices. The analog input signals and the input power are converted to pulse trains and applied to the primary windings, and then they are reconstructed by circuits connected to the transformer secondaries. There are no connections between the input and output circuits, except for the magnetic coupling in the transformers.

Both the analog and the digital signal isolation modules are tested to ensure a minimum isolation potential of 1,500 Vac rms between the input terminals and the output terminals (all input terminals shorted together and all output terminals shorted together), and between the terminals and ground (all terminals shorted together). The 1,500 Vac rms test voltage was applied for at least 60 seconds for each test.

Once generated, any actuation signal remains present until it is manually reset. Each bistable automatically resets when its input signal returns to the "safe" side of the setpoint-deadband region.

IE SB
ITEM 25

reactor when two out of four channels trip becomes a one out of three trip when one channel is placed in the trip mode. Both trains of the logic protection system remain in service during this portion of the test.

2. Check of logic matrices

Logic matrices are checked, one train at a time. Input relays are not operated during this portion of the test. Reactor trips from the train being tested are inhibited with the use of the input error inhibit switch on the semiautomatic test panel in the train. At the completion of the logic matrix tests, one bistable in each channel of process instrumentation or nuclear instrumentation is tripped to check closure of the input error inhibit switch contacts.

The logic test scheme uses pulse techniques to check the coincidence logic. All possible trip and nontrip combinations are checked. Pulses from the tester are applied to the inputs of the universal logic card at the same terminals that connect to the input relay contacts. Thus there is an overlap between the input relay check and the logic matrix check. Pulses are fed back from the reactor trip breaker undervoltage coil to the tester. The pulses are of such short duration that the reactor trip breaker undervoltage coil armature cannot respond mechanically.

Test indications that are provided are an annunciator in the control room indicating that reactor trips from the train have been blocked and that the train is being tested and green and red lamps on the semiautomatic tester to indicate a good or bad logic matrix test. Protection capability provided during this portion of the test is from the train not being tested.

3. General warning alarm reactor trip

Each of the two trains of the solid state protection system is continuously monitored by the general warning alarm reactor trip subsystem. The warning circuits are actuated if undesirable train conditions are set up by improper alignment of testing systems, circuit malfunction or failure, etc., as listed below. A trouble condition in a logic train is indicated in the control room.

I2513
ITEM 25

However, if any of the conditions exist in both trains at the same time, the general warning alarm circuits will automatically trip the reactor.

a. Loss of either of two 48 volt dc or either of two 15 volt dc power supplies.

b. Printed circuit card improperly inserted.

c. Input error inhibit switch in the INHIBIT position.

d. Slave relay tester mode selector in TEST position.

e. Multiplexing selector switch in INHIBIT position.

f. Loss of ac power in relay cabinets.

g. Opposite train bypass breaker racked in and closed.

h. Permissive or memory test switch not in OFF position.

i. Logic function test switch not in OFF position.

The testing capability meets the requirements of GDC-21 (refer to Section 3.1).

Testing of Reactor Trip Breakers

Normally, reactor trip breakers 52/RTA and 52/RTB are in service, and bypass breakers 52/BYA and 52/BYB are withdrawn (out of service). In testing the protection logic, pulse techniques are used to avoid tripping the reactor trip breakers, thereby eliminating the need to bypass them during this testing. The following procedure describes the method used for testing the trip breakers:

IE&B
ITEM 13

The error between the programmed reference temperature (based on turbine impulse chamber pressure) and the highest of the T_{avg} measured temperatures (which is processed through a lead-lag compensation unit) from each of the reactor coolant loops constitutes the primary control signal, as shown in general on Figure 7.7-1 and in more detail on the functional diagrams shown in Figure 7.2-1 (Sheet 9). The system is capable of restoring coolant average temperature to the programmed value following a change in load. The programmed coolant temperature increases linearly with turbine load from zero power to the full power condition. The T_{avg} also supplies a signal to pressurizer level control and steam dump control and rod insertion limit monitoring.

The temperature channels needed to derive the temperature input signals for the reactor control system are fed from protection channels via isolation amplifiers.

An additional control input signal is derived from the reactor power versus turbine load mismatch signal. This additional control input signal improves system performance by enhancing response and reducing transient peaks.

The core axial power distribution is controlled during load follow maneuvers by changing (a manual operator action) the boron concentration in the RCS. The control board $\Delta\phi$ displays (see Section 7.7.1.3.1) indicates the need for an adjustment in the axial power distribution. Adding boron to the reactor coolant will reduce T_{avg} and cause the rods (through the rod control system) to move toward the top of the core. This action will reduce power peaks in the bottom of the core. Likewise, removing boron from the reactor coolant will move the rods further into the core to control power peaks in the top of the core.

7.7.1.2 Rod Control System

7.7.1.2.1 Description

The rod control system receives rod speed and direction signals from the T_{avg} control system. The rod speed demand signal varies over the corresponding range of 3.75 to 45 inches per minute

IE5B
ITEM 93

c. The control bank withdrawals are programmed such that when the first bank reaches a preset position, the second bank begins to move out simultaneously with the first bank which continues to move toward its fully withdrawn position. When the second bank reaches a preset position, the third bank begins to move out, and so on. This withdrawal sequence continues until the unit reaches the desired power level. The control bank insertion sequence is the opposite.

d. Overlap between successive control banks is adjustable between 0 to 50 percent (0 and 115 steps), with an accuracy of ±1 step.

e. Rod speeds for either the shutdown banks or manual operation of the control banks are capable of being controlled between a minimum of 6 steps per minute and a maximum of 72 (+0, -10) steps per minute.

7.7.1.2.2 Features

Credible rod control equipment malfunctions which could potentially cause inadvertent positive reactivity insertions due to inadvertent rod withdrawal, incorrect overlap, or malpositioning of the rods are the following:

a. Failures in the manual rod controls:

   1. Rod motion control switch (in-hold-out)

   2. Bank selector switch

b. Failures in the overlap and bank sequence program control:

   1. Logic cabinet systems

   2. Power supply systems

c. Failures in the manual rod controls

   1. Failure of the rod motion control switch

      The rod motion control switch is a three-position lever switch. The three positions are "In," "Hold," and "Out." These positions are effective when the bank selector switch is in manual. Failure of the rod motion control switch (contacts failing short or activated relay failures) would have the potential, in the worst case, to produce positive reactivity insertion by rod withdrawal when the bank selector switch is in the manual position or in a position which selects one of the banks.

When the bank selector switch is in the automatic position, the rods would obey the automatic commands and failures in the rod motion control switch would have no effect on the rod motion regardless of whether the rod motion control switch is in "In," "Hold," or "Out."

In the case where the bank selector switch is selecting a bank and a failure occurs in the rod motion switch that would command the bank "Out" even when the rod motion control switch was in an "In" or "Hold" position the selected bank could inadvertently withdraw. This failure is bounded in the safety analysis (Chapter 15.0) by the uncontrolled bank withdrawal subcritical and at power transients. A reactivity insertion of up to 75 pcm/sec is assumed in the analysis due to rod movement. This value of reactivity insertion rate is consistent with the withdrawal of two banks.

Failure that can cause more than one group of four mechanisms to be moved at one time within a power cabinet is not a credible event because the circuit arrangement for the movable and lift coils would cause the current available to the mechanisms to divide equally between coils in the two groups (in a power supply). The drive mechanism is designed so that it will not operate on half current. A second feature in this scenario would be the multiplexing failure detection circuit included in each power cabinet. This circuit would stop rod withdrawal (or insertion).

The second case considered in the potential for inadvertent reactivity insertion due to possible failures is when the selector switch is in the manual position. Such a case could produce, with a failure in the rod motion control switch, a scenario where the rods could inadvertently withdraw in a programmed sequence. The overlap and bank sequence are programmed when the selection is in either automatic or manual. This scenario is also bounded by the reactivity values assumed in the SAR accident analysis. In this case, the operator can trip the reactor, or the protection system would trip the reactor via power range neutron flux-high, or overtemperature ΔT.

2. Failure of the bank selector switch

A failure of the bank selector switch produces no consequences when the "in-hold-out" manual switch

Ie 5b
ZIGM 43

is in the "Hold" position. This is due to the following design feature:

The bank selector switch is series wired with the in-hold-out lever switch for manual and individual control rod bank operation. With the in-hold-out lever switch in the "Hold" position, the bank selector switch can be positioned without rod movement.

d. Failures in the overlap and bank sequence program control

The rod control system design prevents the movement of the groups out of sequence as well as limiting the rate of reactivity insertion. The main feature that performs the function of preventing malpositioning produced by groups out of sequence is included in the block supervisory memory buffer and control. This circuitry accepts and stores the externally generated command signals. In the event of out of sequence input command to the rods while they are in movement, this circuit will inhibit the buffer memory from accepting the command. If a change of signal command appears, this circuit would stop the system after allowing the slave cyclers to finish their current sequencing. Failure of the components related to this system will also produce rod deviation alarm and insertion limit alarm. Failures within the system such as failures of supervisory logic cards, pulser cards, etc., will also cause an urgent alarm. An urgent alarm will be followed by the following actions:

Automatic de-energizing of the lift coil and reduced current energizing of the stationary gripper coils and movable grpper coils

Activation of the alarm light (urgent failure) on the power supply cabinet front panel

Activation of rod control urgent failure annunciation window on the plant annunciator

The urgent alarm is produced in general by:

Regulation failure detector

Phase failure detector

Logic error detector

Multiplexing error detector

Interlock failure detector

IE&B
IEM 43

1. Logic cabinet failures

The rod control system is designed to limit the rod speed control signal output to a value that causes the pulser (logic cabinet) to drive the control rod driving mechanism at 72 steps per minute. If a failure should occur in the pulses or the reactor control system, the highest stepping rate possible is 77 steps per minute, which corresponds to one step every 780 milliseconds. A commanded stepping rate higher than 77 steps per minute would result in "GO" pulses entering a slave cycler while it is sequencing its mechanisms through a 780 millisecond step. This condition stops the control bank motion automatically, and alarms are activated locally and in the control room. It also causes the affected slave cycler to reflect further "GO" pulses until it is reset.

Failures that cause the 780 millisecond step sequence time to shorten will not result in higher rod speeds, since the stepping rate is proportional to the pulsing rate. Simultaneous failures in the pulser or rod control system and in the clock circuits that determine the 780 millisecond stepping sequence could result in higher CRDM speed; however, in the unlikely event of these simultaneous multiple failures the maximum CRDM operation speed would be no more than approximately 100 steps per minute due to mechanical limitation. This speed has been verified by tests conducted on the CRDMs.

The positive reactivity insertion rates for these failure modes, including the 100 steps per minute, are bounded by the Chapter 15.0 SAR analysis assumptions.

Failures causing movement of the rods out of sequence:

No single failure was discovered (Ref. 2) that would cause a rapid uncontrolled withdrawal of Control Bank D (taken as worst case) when operating in the automatic bank overlap control mode with the reactor at near full power output. The analysis revealed that many of the failures postulated were in a safe direction and that rod movement is blocked by the rod urgent alarm.

IE SB
IE-M43

2. Power supply system failures

Analysis of the power cabinet disclosed no single component failures that would cause the uncontrolled withdrawal of a group of rods serviced by the power cabinet. The analysis substantiates that the design of a power cabinet is "fail-preferred" with regard to a rod withdrawal accident if a component fails. The end results of the failure is either that of blocking rod movement or that of dropping an individual rod or rods or a group of rods. No failure, within the power cabinet, which could cause erroneous drive mechanism operation will remain undetected. Sufficient alarm monitoring (including "urgent" alarm) is provided in the design of the power cabinet for fault detection of those failures which could cause erroneous operation of a group of mechanisms. As noted in the foregoing, diverse monitoring systems are available for detection of failures that cause the erroneous operation of an individual control rod drive mechanism.

In summary, no single failure within the rod control system can cause either reactivity insertions or mal-positioning of the control rods resulting in core thermal conditions not bounded by analyses contained in Chapter 15.0.

7.7.1.3 Plant Control Signals for Monitoring and Indicating

7.7.1.3.1 Monitoring Functions Provided by the Nuclear Instrumentation System

The power range channels are used to measure power level, axial flux imbalance, and radial flux imbalance. These channels are capable of recording overpower excursions up to 200 percent of full power. Suitable alarms are derived from these signals, as described below.

Basic power range signals are:

a. Total current from a power range detector (four signals from separate detectors); these detectors are vertical and have a total active length of 10 feet.

b. Current from the upper half of each power range detector (four signals).

c. Current from the lower half of each power range detector (four signals).

The following (including standard signal processing for calibration) are derived from these basic signals:

a. Indicated nuclear power (four signals).

b. Indicated axial flux imbalance ($\Delta\phi$), derived from upper half flux minus lower half flux (four signals).

IE SB
ITEM 43

trip from full power. This heat sink is provided by the combination of controlled release of steam to the condenser and by makeup of feedwater to the steam generators.

The steam dump system is controlled from the reactor coolant average temperature signal whose setpoint values are programmed as a function of turbine load. Actuation of the steam dump is rapid to prevent actuation of the steam generator safety valves.

With the dump valves open, the average coolant temperature starts to reduce quickly to the no-load setpoint. A direct feedback of temperature acts to proportionally close the valves to mirimize the total amount of steam which is bypassed.

The feedwater flow is cut off following a reactor trip when the average coolant temperature decreases below a given temperature or when the steam generator water level reaches a given high level.

Additional feedwater makeup is then controlled manually to restore and maintain steam generator water level while assuring that the reactor coolant temperature is at the desired value. Residual heat removal is maintained by the steam header pressure controller (manually selected), which controls the amount of steam flow to the condensers. This controller operates a portion of the same steam dump valves to the condensers, which are used during the initial transient following turbine and reactor trip.

The pressurizer pressure and level fall rapidly during the transient because of coolant contraction. The pressurizer water level is programmed so that the level following the turbine and reactor trip is above the heaters. However, if the heaters become uncovered following the trip, the chemical and volume control system will provide full charging flow to restore water level in the pressurizer. Heaters are then turned on to restore pressurizer pressure to normal.

The steam dump and feedwater control systems are designed to prevent the average coolant temperature from falling below the programmed no-load temperature following the trip to ensure adequate reactivity shutdown margin.

7.7.3 REFERENCES

1. Lipchak, J. B., "Nuclear Instrumentation System," WCAP-8255, January, 1974. (For additional background information only.)

2. Shopsky, W. E., "Failure Mode and Effects Analysis (FMEA) of the Solid State Full Length Rod Control System," WCAP-8976, August 1977.

TABLE 1.6-2 (Sheet 16)

Westinghouse Topical Report No.	Title	Revision Number	FSAR Section Reference	Report Submitted to the NRC	Review Status (1)
WCAP-8872	"Design, Inspection, Operation and Maintenance Aspects of the Westinghouse NSSS to Maintain Occupational Radiation Exposures as Low as Reasonably Achievable."	Rev. 0	12.1	4/27/77	B
WCAP-8892-A	"Westinghouse 7300 Series Process Control System Noise Tests"	Rev. 0	7.1	6/15/77	A
WCAP-8929	"Benchmark Problem Solutions Employed for Verification of the WECAN Computer Program"	Rev. 0	3.9(N)	5/26/77	U
WCAP-8963 (P) WCAP-8964	"Safety Analysis for the Revised Fuel Rod Internal Pressure Design Basis"	Rev. 0	4.2	3/31/77 8/11/77	A
WCAP-8976	"Failure Mode and Effects Analysis (FMEA) of the Solid State Full Length Rod Control System"	Rev. 0	4.6, 7.7	10/26/77	U
WCAP-9168 (P) WCAP-9150	"Westinghouse Emergency Core Cooling System Evaluation Model - Modified October 1975 Version"	Rev. 0	15.6	9/27/77	U
WCAP-9179 (P)	"Properties of Fuel and Core Component Materials"	Rev. 1	4.2	8/2/78	U

ICSB
ITEM 46

15.3.2 COMPLETE LOSS OF FORCED REACTOR COOLANT FLOW

15.3.2.1 Identification of Causes and Accident Description

A complete loss of flow accident may result from a simultaneous loss of electrical supplies to all reactor coolant pumps. If the reactor is at power at the time of the accident, the immediate effect of loss-of-coolant flow is a rapid increase in the coolant temperature. This increase could result in a DNB with subsequent fuel damage if the reactor were not tripped promptly.

Normal power for the reactor coolant pumps is supplied through busses from a transformer connected to the generator. When a generator trip occurs, the busses are automatically transferred to a transformer supplied from external power lines, and the pumps will continue to supply coolant flow to the core. Following any turbine trip where there are no electrical faults which require tripping the generator from the network, the generator remains connected to the network for approximately 30 seconds. The reactor coolant pumps remain connected to the generator, thus ensuring full flow for 30 seconds after the reactor trip before any transfer is made.

A complete loss of flow accident is classified as an ANS Condition III event (an infrequent fault), as defined in Section 15.0.1. The following signals provide protection against this event:

a. Reactor coolant pump power supply undervoltage or underfrequency
b. Low reactor coolant loop flow

The reactor trip on reactor coolant pump undervoltage is provided to protect against conditions which can cause a loss of voltage to all reactor coolant pumps, i.e., station blackout. This function is blocked below approximately 10-percent power (Permissive 7).

The reactor trip on reactor coolant pump underfrequency is provided to trip the reactor for an underfrequency condition, resulting from frequency disturbances on the power grid. Reference 3 provides analyses of grid frequency disturbances and the resulting NSSS protection requirements which are applicable to the SNUPPS units.

Reference 3 shows that the underfrequency trip of the reactor coolant pump breakers is not required for grid decay rates up to 5 hz/sec. Grid stability and transient analyses for both the Wolf Creek and Callaway sites show maximum grid decay rates of less than 5 hz/sec. Therefore, the reactor coolant pump breaker trip on under frequency (Figure 7.2-1, Sheet 5) is not a safety function in the SNUPPS design.

IE SB
ITEM 6

The reactor trip on low primary coolant loop flow is provided to protect against loss of flow conditions which affect only one reactor coolant loop. This function is generated by two out of three low flow signals per reactor coolant loop. Above Permissive 8, low flow in any loop will actuate a reactor trip. Between approximately 10-percent power (Permissive 7)

IE SB
ITEM 48

7.1.2.1 Design Bases

The design bases for the safety-related systems are provided in the respective sections of Chapter 7.0.

7.1.2.2 Independence of Redundant Safety-Related Systems

The safety-related systems are designed to meet the independence and separation requirements of GDC-22 and Section 4.6 of IEEE Standard 279-1971.

The electrical power supply, instrumentation, and control conductors for redundant circuits of a nuclear plant have physical separation to preserve the redundancy and to ensure that no single credible event will prevent operation of the associated function. Critical circuits and functions include power, control, and analog instrumentation associated with the operation of the safety-related systems. Events considered credible and considered in the design include the effects of short circuits, pipe rupture, missiles, and fire.

7.1.2.2.1 General

The physical separation criteria for redundant safety-related system sensors, sensing lines, wireways, cables, and components on racks meet the recommendations contained in Regulatory Guide 1.75 with the following comments:

a. The protection systems use redundant instrumentation channels and actuation trains and incorporate physical and electrical separation to prevent faults in one channel from degrading any other protection channel.

b. Where no redundant circuits share a single compartment of a safety-related instrumentation rack and these redundant safety-related instrumentation racks are physically separated, the recommendations of Position C.16 of Regulatory Guide 1.75 do not apply.

c. Redundant, isolated control signal cables leaving the protection racks are brought into close proximity elsewhere in the plant, such as the control board. It could be postulated that electrical faults, or interference, at these locations might be propagated into all redundant racks and degrade protection circuits because of the close proximity of protection

ICSB
ITEM 48

and control wiring within each rack. Regulatory Guide 1.75 (Regulatory Position C.4) and IEEE Standard 384-1974 (Section 4.5(3)) provide the option to demonstrate by tests that the absence of physical separation could not significantly reduce the availability of Class IE circuits.

Westinghouse test programs have demonstrated that Class IE protection systems (nuclear instrumentation system, solid state protection system, and 7300 process control system) are not degraded by non-Class IE circuits sharing the same enclosure. Conformance to the requirements of IEEE Standard 279-1971 and Regulatory Guide 1.75 has been established and accepted by the NRC, based on the following which is applicable to these systems at the SNUPPS sites.

Tests conducted on the as-built designs of the nuclear instrumentation system and solid state protection system were reported and accepted by the NRC in support of the Diablo Canyon application (Docket Nos. 50-275 and 50-323). Westinghouse considers these programs as applicable to all plants, including SNUPPS. Westinghouse tests on the 7300 process control system were covered in a report entitled, "7300 Series Process Control System Noise Tests," subsequently reissued as Reference 2. In a letter dated April 20, 1977 (Ref. 3), the NRC accepted the report in which the applicability of the SNUPPS plants is established.

d. The physical separation criteria for instrument cabinets within the NSSS scope meet the recommendations contained in Section 5.7 of IEEE Standard 384-1974. Compliance with specific positions of Regulatory Guide 1.75 is given in Chapter 8.0.

7.1.2.2.2 Specific Systems

Independence is maintained throughout each system, extending from the sensor through to the devices actuating the protective function. Physical separation is used to achieve separation of redundant transmitters. Separation of field wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant protection channel set. Redundant analog equipment is separated by locating modules in different protection rack sets. Each redundant channel set is energized from a separate ac power feed.

There are four separate protection sets. Each protection set contains several channels, each channel sensing a different variable. Separation of redundant analog channels begins at the process sensors and is maintained in the field wiring,