


BEAVER VALLEY UNIT 2
FAILURE OF FEEDWATER CONTROL
CHANNEL USED FOR PROTECTION

T. A. Blackburn

February 1984

Approved:


J. L. Little, Manager
Transient Analysis

Westinghouse Electric Corporation
Nuclear Energy Systems
P.O. Box 355
Pittsburgh, Pennsylvania 15230

TABLE OF CONTENTS

<u>Section</u>	<u>Title</u>
1.0	Purpose of Analysis
2.0	Background
3.0	Description of the Event
4.0	Transient Results
5.0	Conclusions
6.0	References

LIST OF TABLES

<u>Table</u>	<u>Title</u>
1	Initial Conditions
2	Time Sequence of Events for a Feedwater Control Malfunction With Reactor Trip
3	Time Sequence of Events for a Feedwater Control Malfunction Without a Reactor Trip
4	Time Sequence of Alarms and Annunciators for a Feedwater Control Malfunction With a Reactor Trip
5	Time Sequence of Alarms and Annunciators for a Feedwater Control Malfunction Without a Reactor Trip

LIST OF FIGURES

<u>Figure</u>	<u>Title</u>
1	Steam Generator 1 Level Logic
2	Steam Generator 1 Initiating Event
3	Steam Generator 1 Case 1 Single Active Failure
4	Steam Generator 1 Case 2 Single Active Failure
5	Feedwater Control Malfunction Nuclear Power and Core Heat Flux versus Time No Reactor Trip (Beginning of Core Life)
6	Feedwater Control Malfunction RCS Average Temperature, Delta T and Pressurizer Pressure versus Time No Reactor Trip (Beginning of Core Life)
7	Feedwater Control Malfunction Steam Generator Secondary Side Volume and DNB Ratio versus Time No Reactor Trip (Beginning of Core Life)
8	Feedwater Control Malfunction Nuclear Power and Core Heat Flux versus Time No Reactor Trip (End of Core Life)
9	Feedwater Control Malfunction RCS Average Temperature, Delta T and Pressurizer Pressure versus Time No Reactor Trip (End of Core Life)
10	Feedwater Control Malfunction Steam Generator Secondary Side Volume and DNB Ratio versus Time No Reactor Trip (End of Core Life)
11	Feedwater Control Malfunction Nuclear Power and Core Heat Flux versus Time Reactor Trip on Lo-Lo Steam Generator Level (Beginning of Core Life)

LIST OF FIGURES (Cont)

<u>Figure</u>	<u>Title</u>
12	Feedwater Control Malfunction RCS Average Temperature Delta T and Pressurizer Pressure versus Time Reactor Trip Lo-Lo Steam Generator Level (Beginning of Core Life)
13	Feedwater Control Malfunction Steam Generator Secondary Side Volume and DNB Ratio versus Time Reactor Trip on Lo-Lo Steam Generator Level (Beginning of Core Life)
14	Feedwater Control Malfunction Nuclear Power and Core Heat Flux versus Time Reactor Trip on Lo-Lo Steam Generator Level (End of Core Life)
15	Feedwater Control Malfunction RCS Average Temperature, Delta T and Pressurizer Pressure versus Time Reactor Trip on Lo-Lo Steam Generator Level (End of Core Life)
16	Feedwater Control Malfunction Steam Generator Secondary Side Volume and DNB Ratio versus Time Reactor Trip on Lo-Lo Steam Generator Level (End of Core Life)

1.0 PURPOSE OF ANALYSIS

The Instrumentation and Control Systems Branch of the United States Nuclear Regulatory Commission has questioned Beaver Valley Power Station Unit 2 in regards to feedwater isolation. More specifically, the issue has been raised of strictly applying single failure criteria to two out of three hi-hi steam generator water level logic for feedwater isolation.

The purpose of this analysis is to justify the adequacy of the current design. This report describes the expected transient performance of Beaver Valley Unit 2 for several postulated scenarios. It demonstrates that no unacceptable consequences occur.

2.0 BACKGROUND

A safety analysis of Feedwater System Malfunction Causing an Increase in Feedwater Flow is presented in the Beaver Valley Unit 2 Final Safety Analysis Report. It demonstrates that the Departure from Nucleate Boiling (DNB) design basis is met for that accident. Therefore, DNB is not a safety concern here.

It should be pointed out that one of the assumptions in the FSAR analysis is feedwater isolation on a hi-hi steam generator level signal. However, the DNB ratio (DNBR) reached its minimum and had begun to increase prior to feedwater isolation. Therefore, even without taking credit for the hi-hi level signal, the DNB design basis would have been met.

The single random failure requirement of IEEE-279 stipulates that where a random failure can result in a control system action that produces a plant condition requiring protective action, and simultaneously prevents the proper action of a protection channel designed to protect against that plant condition, the remaining redundant channels shall be capable of protecting the plant even when degraded by a second random failure. As regards the steam generator level signal, if the transmitter in the level channel used for control purposes fails in such a way as to cause high feedwater flow (and increasing level), a subsequent failure in one of the two remaining channels might prevent the actuation of feedwater isolation.

Feedwater isolation is normally actuated by a hi-hi steam generator water level signal in any one of the three steam generators. In each steam generator, hi-hi level signal is based upon receiving the indication in 2 out of 3 channels.

Figure 1 will facilitate the following discussion. 2 of the 3 steam generator water level channels in each steam generator have bistables for each of the following three functions: lo-lo steam generator water level reactor trip, low steam generator water level signal for low feedwater flow reactor trip, and hi-hi steam generator water level turbine trip and feedwater isolation. The third channel replaces low steam generator water level signal with input to the appropriate feedwater control valve.

The following scenario has been postulated. If for some reason the transmitter in this third channel were to fail low, the feedwater control valve would begin to open, to keep the steam generator water level near its setpoint. Strictly applying the single active failure criteria (failure in one of the other two SG water level channels), the hi-hi steam generator water level signal could not be generated in that loop. Only one channel is available to indicate water level above hi-hi, but 2 are needed for the logic. Thus this function, hi-hi steam generator water level turbine trip and feedwater isolation which was assumed in the FSAR, is not available.

However, if one considers the actual performance of the plant and the other protective functions, it can be demonstrated that the event has no unacceptable consequences.

3.0 DESCRIPTION OF EVENT

This excessive feedwater flow transient is initiated by a feedwater control failure. It is exacerbated by a subsequent protective system failure. This failure precludes the actuation of the function, feedwater isolation on hi-hi steam generator level, which is assumed in the Final Safety Analysis Report.

Figure 1 displays the logic of the level signals in steam generator 1 (used as an example). Four functions are provided: lo-lo level reactor trip, low level for low feedwater reactor trip and hi-hi level turbine trip and feedwater isolation, protective functions, and feedwater control, a control function. Each protective function requires two out of three bistables actuated to perform. (Low level must be in coincidence with steam flow/feed flow mismatch, but requires only one out of two channels). A dedicated channel is used in feedwater control. It continuously indicates position, rather than a range.

Figure 2 shows the same logic after the initiating event. The transmitter in channel III falls low. A lo-lo level signal is generated in that channel; hi-hi level is not. The Feedwater Control System tells the valve to open.

Figures 3 and 4 take this one step further - the single active failure is incorporated. Figure 3 assumes that the failure causes another channel to believe its level is also at the bottom. Therefore a second lo-lo signal is generated and the reactor is tripped. This is the first case to be analyzed.

Figure 4 assumes that the failure restrains channel I from generating any signal. The third channel (II) will operate properly above nominal (single failure already assumed). However, no other channels will be able to indicate level above the hi-hi setpoint. Channel I has no signal and Channel III indicates below lo-lo level. Therefore, none of the three protective functions will be actuated. This is the second case.

If the failure were to produce a hi-hi level signal in that channel, turbine trip and feedwater isolation would occur when the level in the third (unfaulted) channel reaches the hi-hi level setpoint. This is consistent with the FSAR analysis.

The excessive heat removal due to a feedwater system malfunction transient is analyzed by using the detailed digital computer code LOFTRAN (Burnett 1972). This code simulates a multi-loop system, the neutron kinetics, the pressurizer, pressurizer relief and safety valves, pressurizer spray, steam generator, and steam generator safety valves. The code computes pertinent plant variables including temperatures, pressures, and power level.

A control system malfunction is assumed to cause a feedwater control valve to open fully. Two cases are analyzed as follows:

1. Opening of one feedwater control valve with the reactor at full power. Reactor trip is generated lo-lo steam generator water level in 2 out of 3 channels. (One channel failing low initiates the transient; the second channel failing low is the single active failure.)
2. Accidental opening of one feedwater control valve with the reactor at full power without consideration of reactor trip.

Each of these cases is analyzed for both beginning of life and end of life core conditions.

The following assumptions have been made:

1. One indicated steam generator water level signal used for control is assumed to fail in such a way as to indicate zero level and demand full feedwater flow.
2. Feedwater flow rate is automatically controlled through the Steam Generator Level Control System using indicated steam flow, feedwater flow, steam generator water level and a programmed level setpoint.

3. Steam flow at its full load value until turbine trip (one second after reactor trip).
4. The Pressurizer Pressure Control System functions normally.
5. The Steam Dump Control System functions.
6. No credit is taken for the heat capacity of the RCS and steam generator thick metal in attenuating the resulting plant cooldown.
7. Feedwater isolation on hi-hi steam generator water level signal is defeated.
8. The feedwater flow is isolated after reactor trip by a low T_{avg} signal in two out of three loops.
9. Initial operating conditions are assumed at values consistent with steady-state operation. Refer to Table 1.

No other reactor control systems or engineered safety feature (ESF) systems are required to function. The reactor protection system (RPS) will function to trip the reactor due to overpower or over temperature conditions. No single active failure will prevent operation of the RPS.

4.0 TRANSIENT RESULTS

The first case analyzed proceeds in the following manner. The steam generator level transmitter used for level control fails low. This causes the control system to open the feedwater control valve in an attempt to restore level to its programmed value. Also, the failed transmitter generates a 10-10 level reactor trip signal in that channel.

A subsequent single active failure of a second level channel produces 10-10 and low level signals in one of the other two channels. A reactor trip is generated on a 2 out of 3 coincidence of 10-10 steam generator level (Figure 3).

At this point, reactor trip initiates turbine trip and the Steam Dump Control System is actuated to reduce primary temperature to the no-load valve.

The increasing saturation pressure and decreasing temperature in the steam generator due to reduced heat transfer causes the secondary side steam generator mixture to collapse. This "shrink" results in a reduced mixture volume and level of the steam generator secondary side.

When the average RCS temperature in two out of three loops reaches the low T_{avg} set point (no load plus 7°F) in coincidence with the P-4 permissive (tripped reactor) all feedwater control valves begin to close. This prevents further addition of main feedwater.

Transient results (Figures 5 through 10) show the nuclear power, core heat flux, average RCS temperature, loop delta-T, pressurizer pressure, steam generator water volume and DNB ratio for this case. The steam generator water level reaches a peak of only 40 percent of the narrow range span which is less than the initial value. Therefore, the steam generator will not overflow. Table 2 presents a sequence of events for this transient.

The second case is initiated exactly as the first case is. However, its subsequent single failure is assumed to be a failure of the transmitter at its previous value. Reactor trip does not occur (Figure 4). The purpose of this case is to determine the amount of time available for the operator to terminate this event prior to overflow.

This transient has a very minor impact upon the plant. The only parameter that significantly changes is steam generator water volume, which slowly and steadily increases.

Transient results (Figures 11 through 16) show the nuclear power, core heat flux, average RCS temperature, loop delta-T, pressurizer pressure, steam generator water volume, and DNB ratio. The steam generator water volume does not exceed the capacity of the secondary side, 5760 cubic feet, within the first ten minutes.

From Figures 13 and 16, one can see that approximately ten minutes are available for the operator to isolate feedwater before steam generator overfill could occur. Table 5 contains a listing of alarms and annunciators which would actuate as a result of this transient.

Considering that this is not a complex transient and is very easily diagnosed and is often a standard malfunction used in reactor operator training courses, it is apparent that this ten minute time span for operator action is sufficient. This assumption is entirely consistent with those made in other safety analyses in the Beaver Valley Unit 2 FSAR.

5.0 CONCLUSIONS

The analysis presented in the Beaver Valley Unit 2 FSAR has demonstrated that there is adequate core protection against DNB for excessive feedwater flow transients.

In addition, these analyses have shown that, when one considers the transient response including the actuation of other protective functions, the protection and control systems design of Beaver Valley Unit 2 provides adequate protection against excessive feedwater flow transients from a steam generator overfill viewpoint.

6.0 REFERENCES

Burnett, T. W. T., et al 1972. LOFTRAN Code Description. WCAP-7907, June, 1972. Also supplementary information in letter from T. M. Anderson, NS-TMA-1802, May 26, 1978 and NS-TMA-1824, June 16, 1978.

Beaver Valley Power Station Unit 2, Final Safety Analysis Report.

TABLE 1

INITIAL CONDITIONS

Core Power, MWt	2660
Thermal Design Flow, GPM	265500
Reactor Coolant Average Temperature, °F	576.2
Reactor Coolant System Pressure, psia	2250
Steam Generators Secondary Side Volume, ft ³	3420

TABLE 2

TIME SEQUENCE OF EVENTS FOR A FEEDWATER
CONTROL MALFUNCTION WITH REACTOR TRIP

<u>Accident</u>	<u>Event</u>	<u>Time (sec)</u>
1. Beginning of Life Core Conditions	Feedwater Control Valve begins to open, loop 1	0
	Lo-lo SG level reactor trip	0
	Minimum DNBR occurs	0
	Turbine trip on reactor trip	1
	Low T_{avg} reached, loops 1 and 3	7
	Feedwater control valves fully closed	14
	2. End of Life Core Conditions	Feedwater Control Valve begins to open, loop 1
Lo-lo SG level reactor trip	0	
Minimum DNBR occurs	0	
Turbine trip on reactor trip	1	
Low T_{avg} reached, loops 1 and 3	8	
Feedwater control valves fully closed	15	

TABLE 3

TIME SEQUENCE OF EVENTS FOR A FEEDWATER
CONTROL MALFUNCTION WITHOUT REACTOR TRIP

<u>Accident</u>	<u>Event</u>	<u>Time (sec)</u>
1. Beginning of Life Core Conditions	Feedwater Control Valve begins to open, loop 1	0
	Minimum DNBR occurs	0
	Hi-hi SG level reached, loop 1	143
	Water reaches top of SG, loop 1	>600
2. End of Life Core Conditions	Feedwater Control Valve begins to open, loop 1	0
	Minimum DNBR occurs	0
	Hi-hi SG level reached, loop 1	146
	Water reaches top of SG, loop 1	>600

TABLE 4

TIME SEQUENCE OF ALARMS AND ANNUNCIATORS FOR
A FEEDWATER CONTROL MALFUNCTION WITH REACTOR TRIP

<u>Accident</u>	<u>Event</u>	<u>Time (sec)</u>
1. Beginning of Life Core Conditions	Bistable 474 A	0
	Bistable 476 A	0
	Channel 474, 10-10 SG level	0
	Channel 476, 10-10 SG level	0
	Reactor tripped	0
	Low level deviation alarm	0
	Steam dump valves open	2
	Low T_{avg} interlock	7
	Feedwater Control Valves fully closed	14
2. End of Life Core Conditions	Bistable 474 A	0
	Bistable 476 A	0
	Channel 474, 10-10 SG level	0
	Channel 476, 10-10 SG level	0
	Reactor tripped	0
	Low level deviation alarm	0
	Steam dump valves open	2
	Low T_{avg} interlock	8
	Feedwater Control Valves fully closed	15

TABLE 5

TIME SEQUENCE OF ALARMS AND ANNUNCIATORS FOR A
FEEDWATER CONTROL MALFUNCTION WITHOUT REACTOR TRIP

<u>Accident</u>	<u>Event</u>	<u>Time (sec)</u>
1. Beginning of Life Core Conditions	Bistable 476 A	0
	Channel 476, lo-lo SG level	0
	Low level deviation alarm	0
	Feedwater Control Valve fully open, loop 1	9
	Channel 475, hi-hi SG level	143
	Bistable 475C	143
	2. End of Life Core Conditions	Bistable 476 A
Channel 476, lo-lo SG level		0
Low level deviation alarm		0
Feedwater Control Valve fully open, loop 1		9
Channel 475, hi-hi SG level		146
Bistable 475C		146

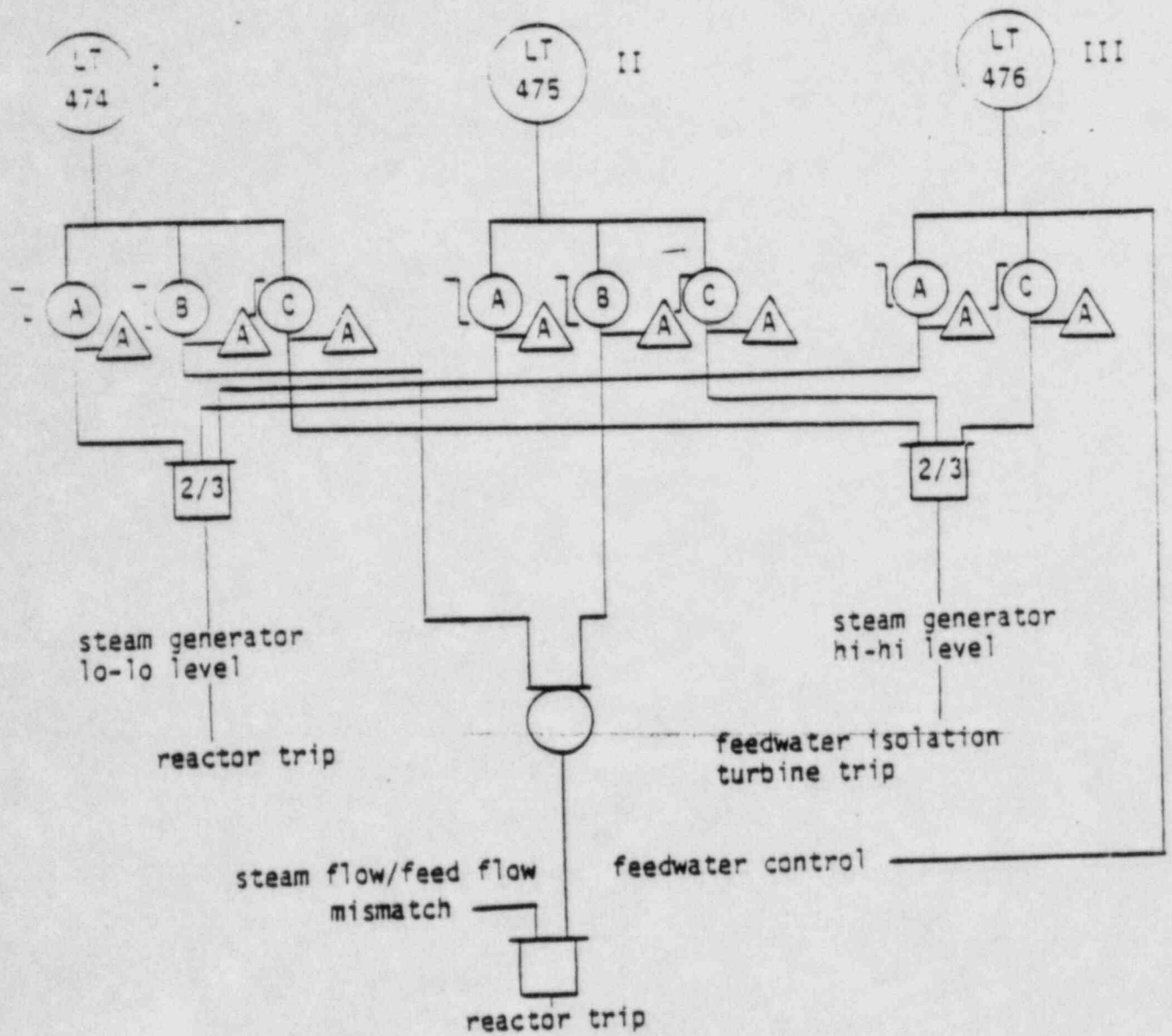
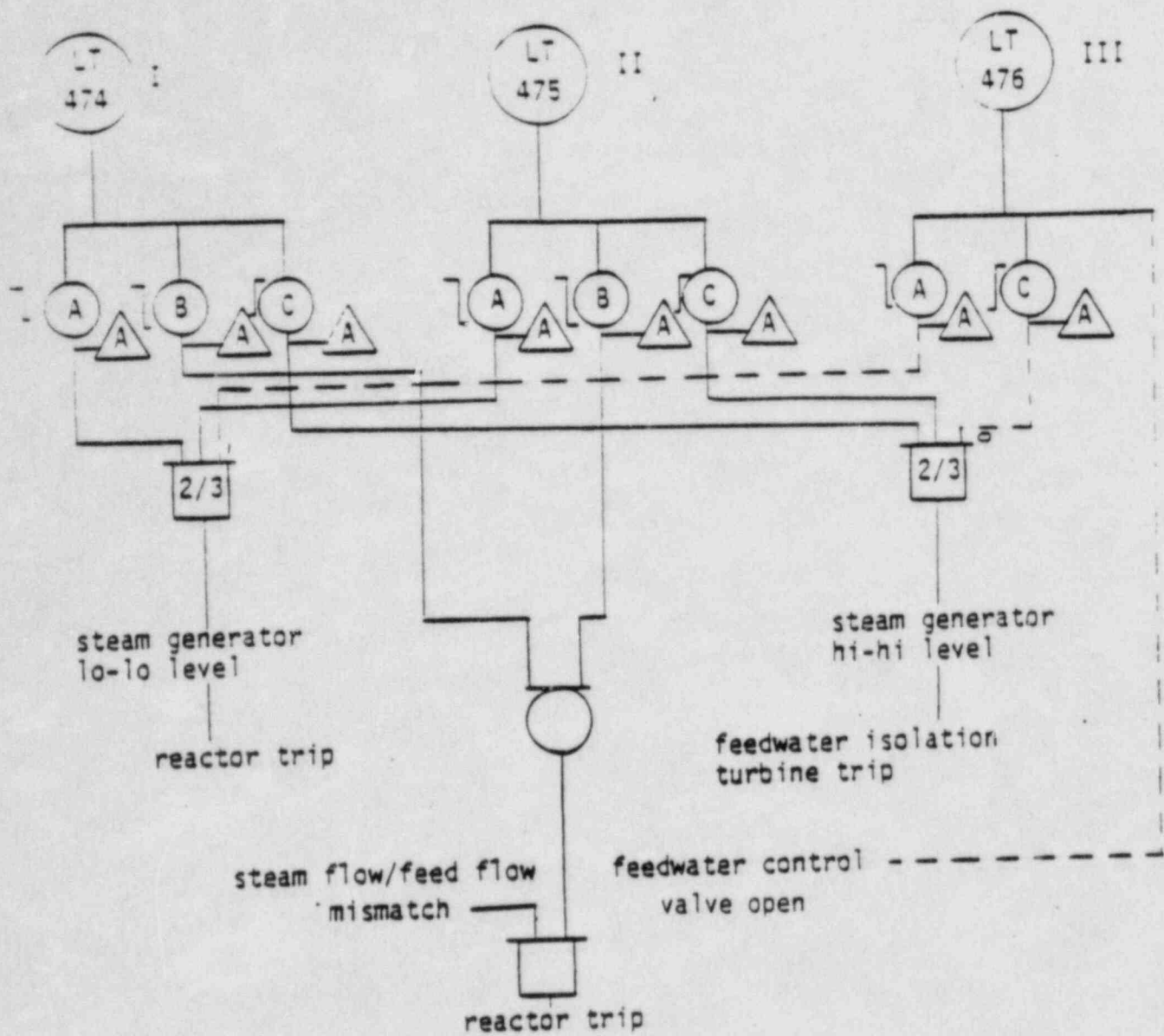


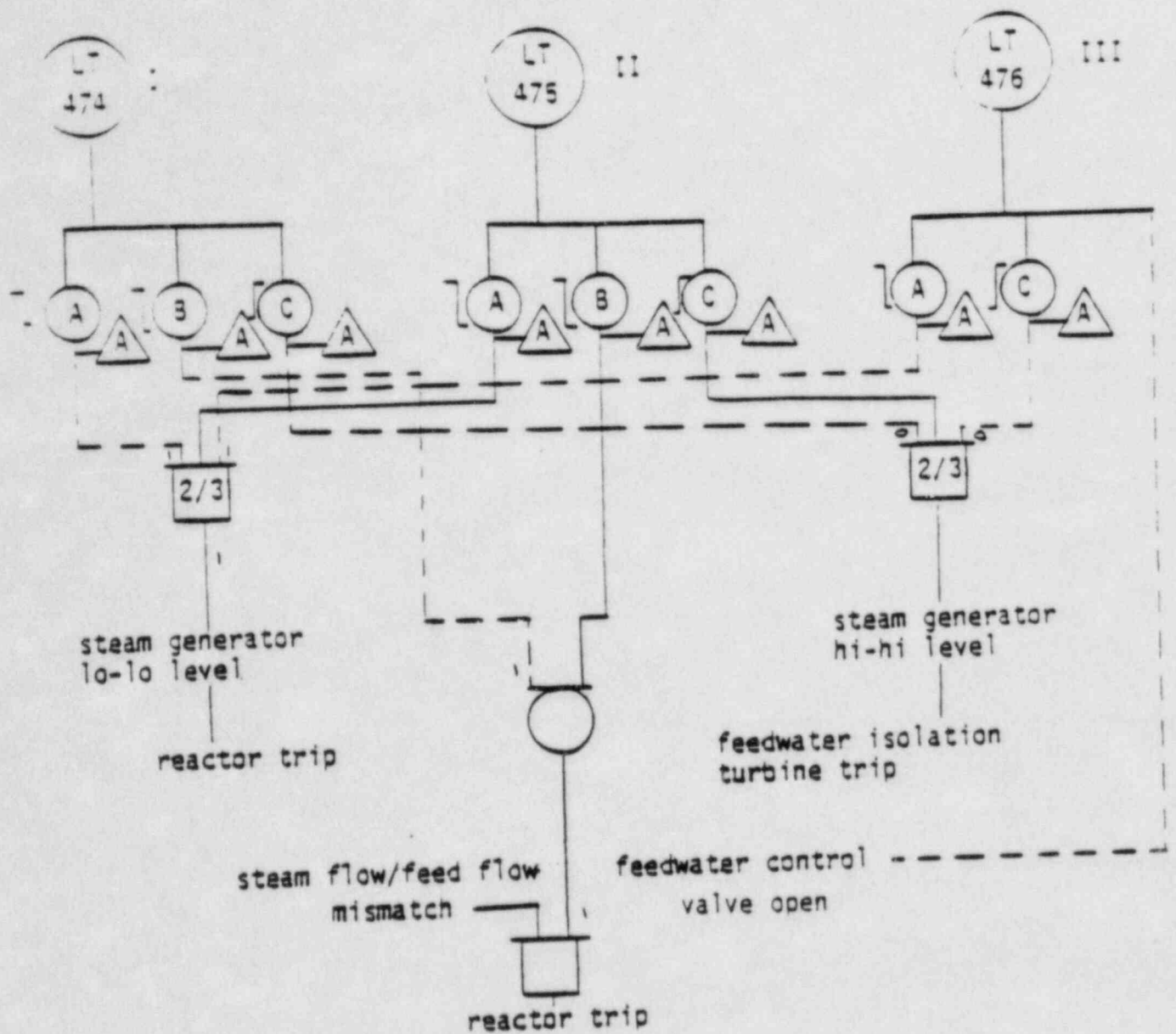
FIGURE 1

STEAM GENERATOR 1 LEVEL LOGIC



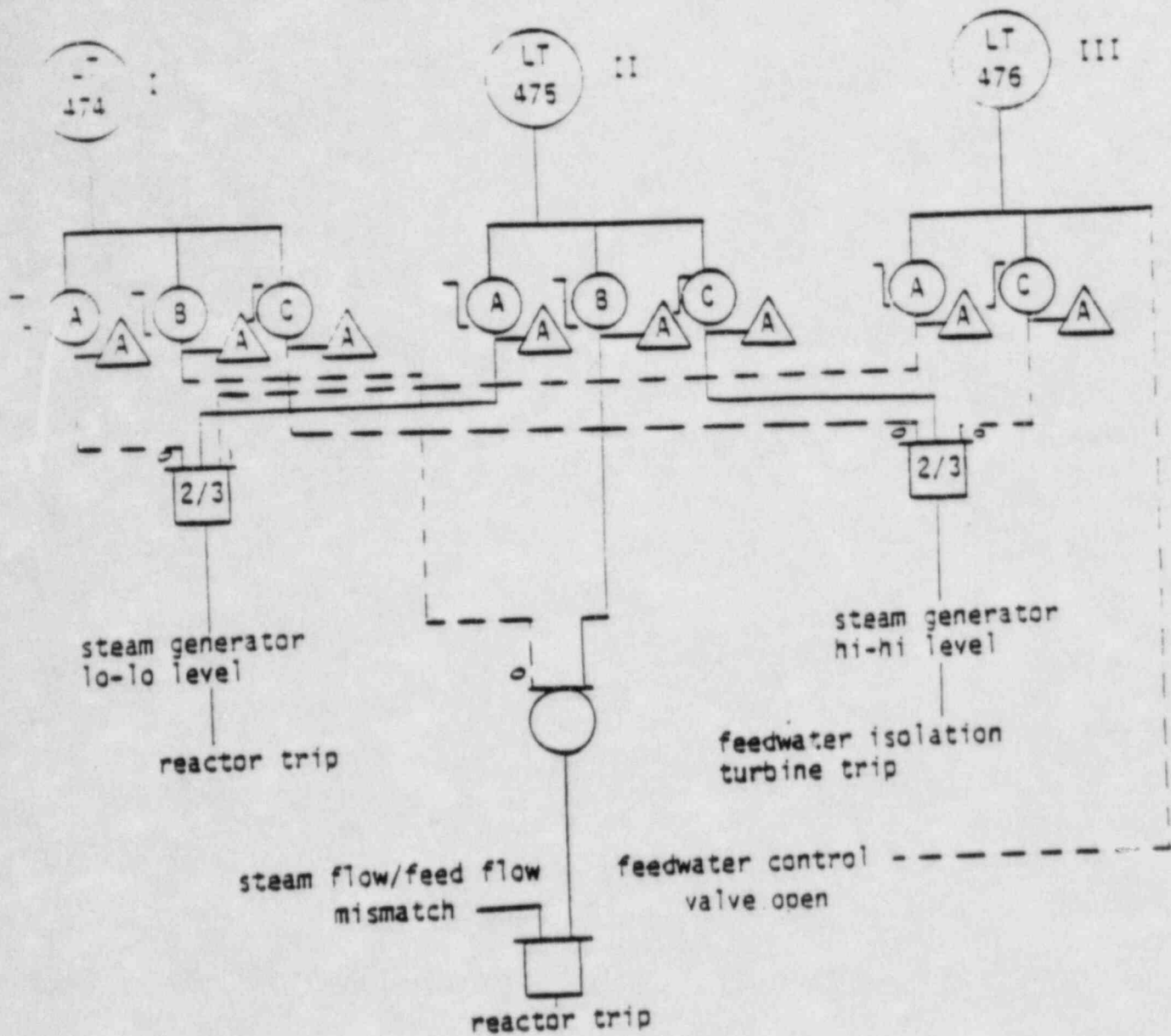
Level transmitter 476 fails low, causing the FCV to open fully, the 10-10 level signal to be sent and the hi-hi signal to be withheld.

FIGURE 2
STEAM GENERATOR 1 INITIATING EVENT



Level transmitter 474 fails low, sending out lo-lo and low level signals and withholding the hi-hi signal. Reactor trip on lo-lo level is generated.

FIGURE 3
 STEAM GENERATOR 1
 CASE 1 SINGLE ACTIVE FAILURE



Channel 474 fails as is, thereby generating no signals.

FIGURE 4
 STEAM GENERATOR 1
 CASE 2 SINGLE ACTIVE FAILURE

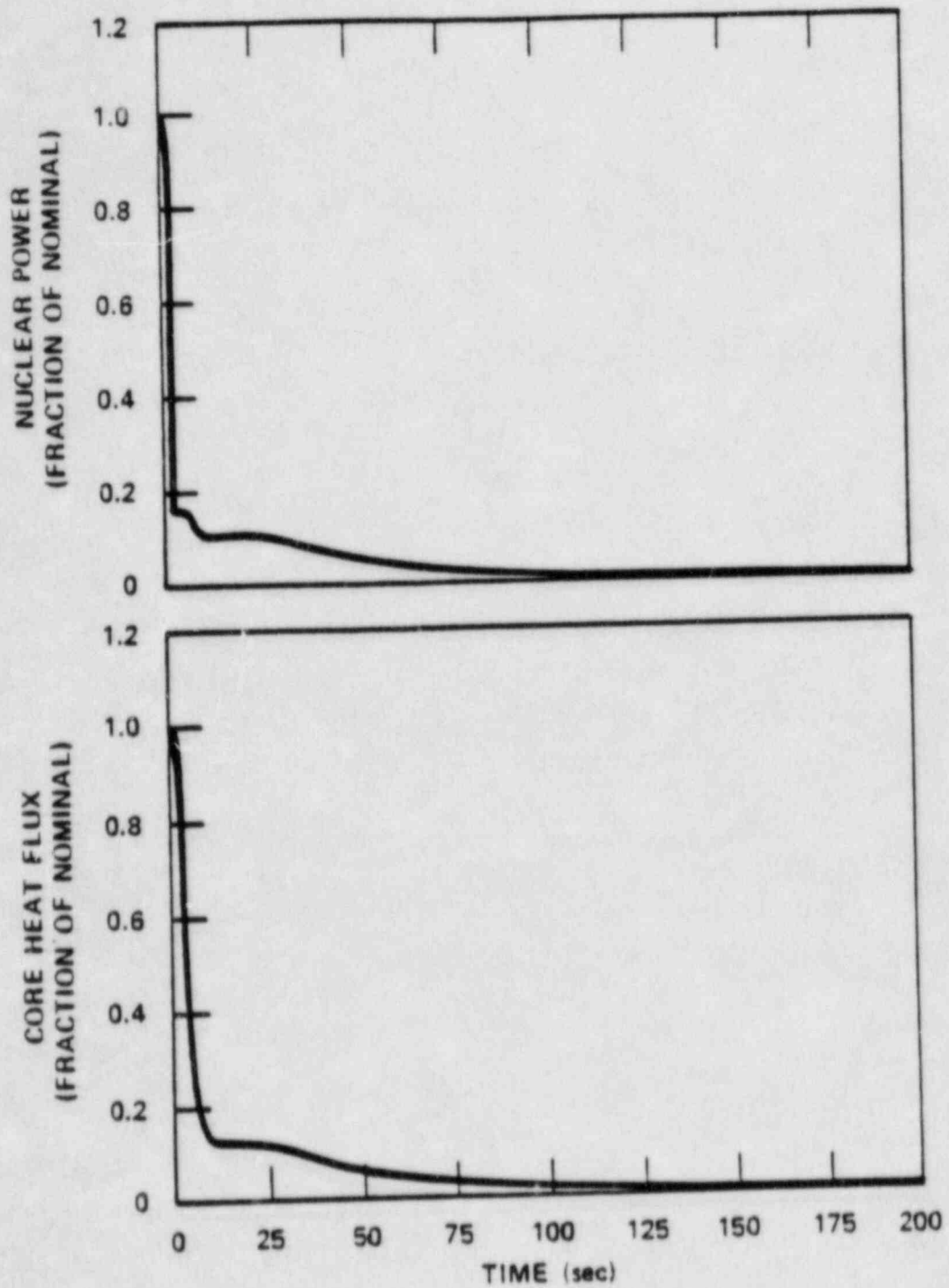


Figure 5. Feedwater Control Malfunction Nuclear Power and Core Heat Flux versus Time Reactor Trip on Lo-Lo Steam Generator Level (Beginning of Core Life)

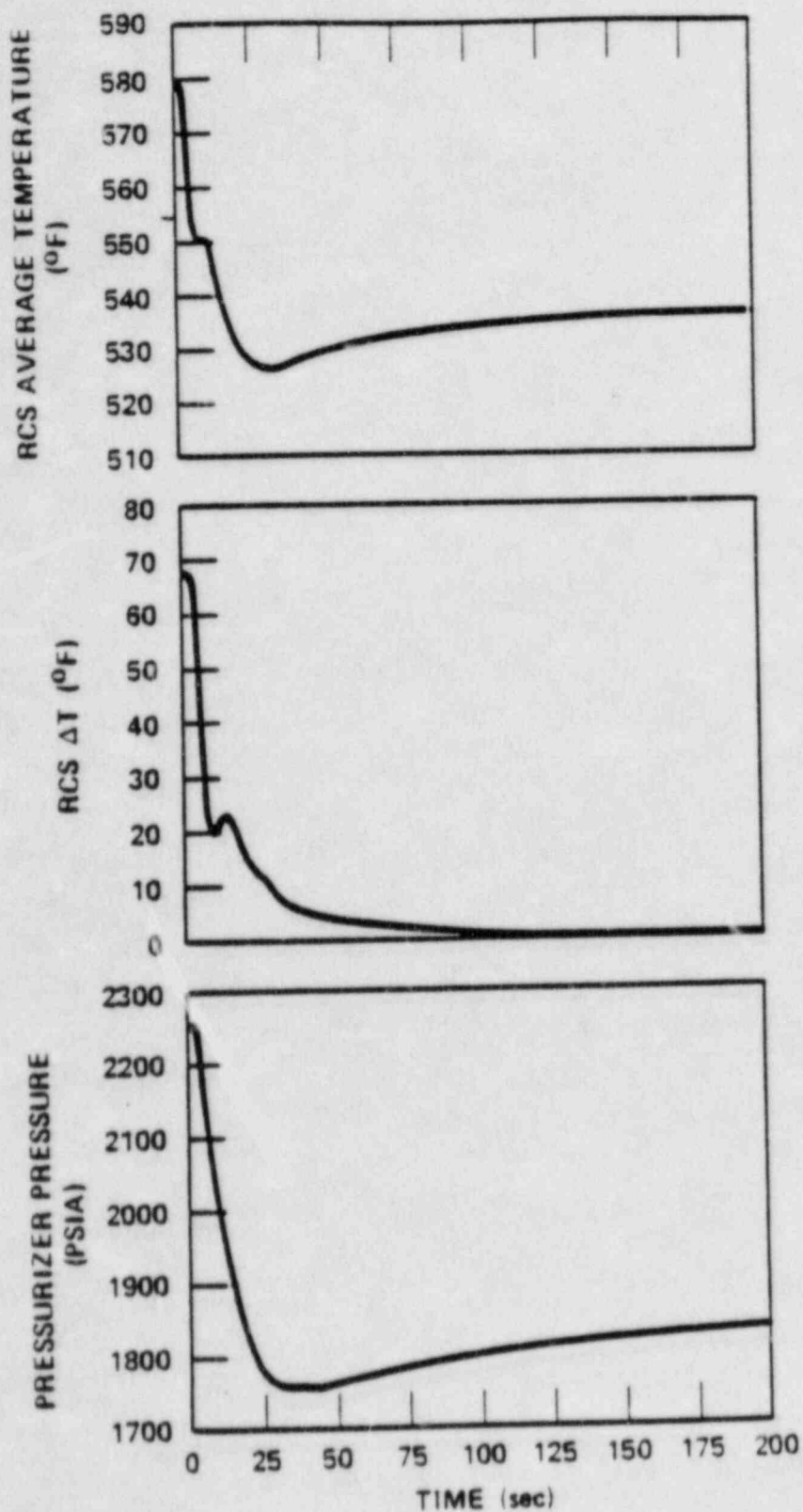


Figure 6. Feedwater Control Malfunction RCS Average Temperature, ΔT and Pressurizer Pressure Versus Time Reactor Trip on "Lo-Lo Steam Generator Level (Beginning of Core Life)

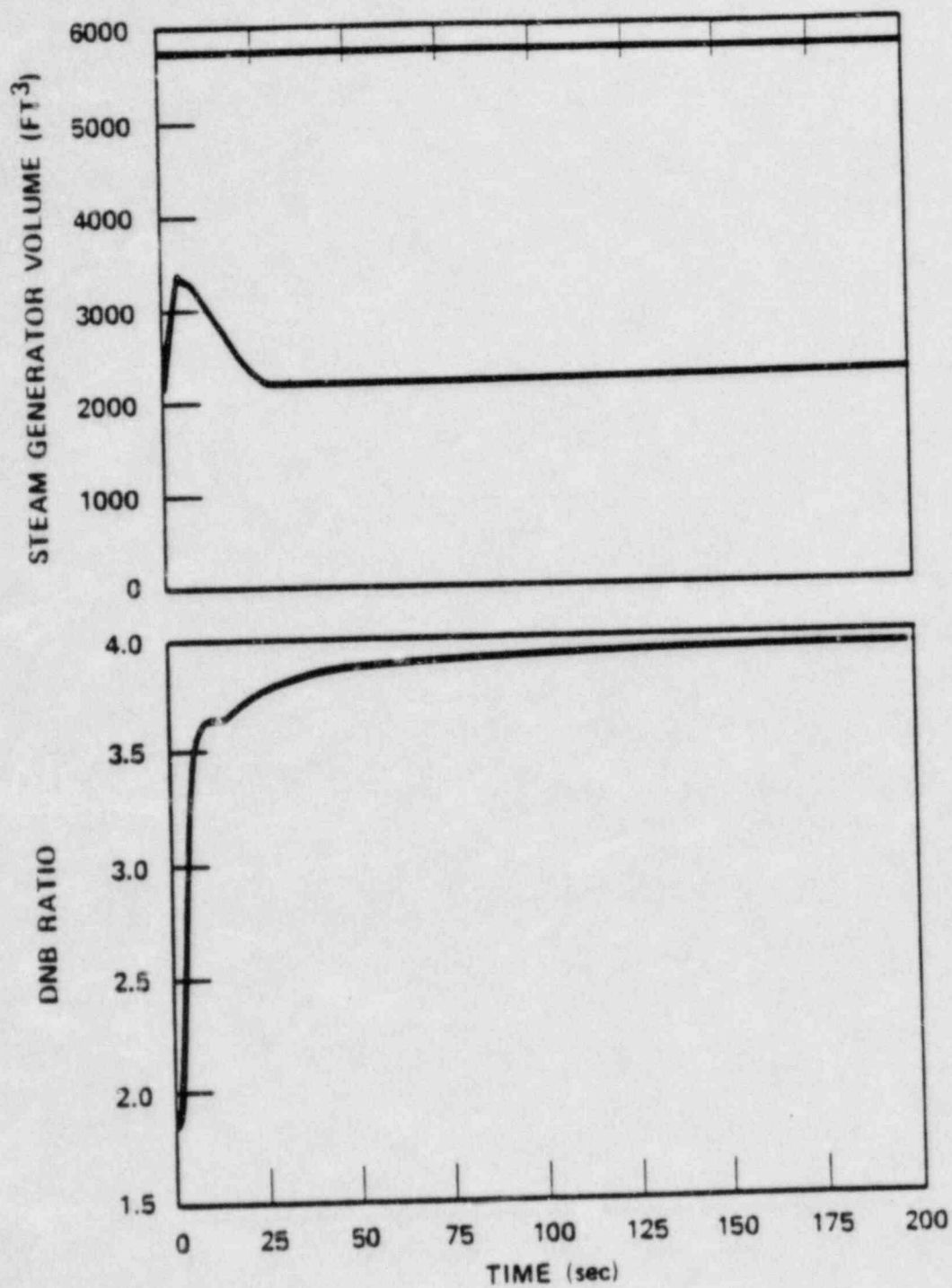


Figure 7. Feedwater Control Malfunction Steam Generator Secondary Side Volume and DNB Ratio Versus Time Reactor Trip on Lo-Lo Steam Generator Level (Beginning of Core Life)

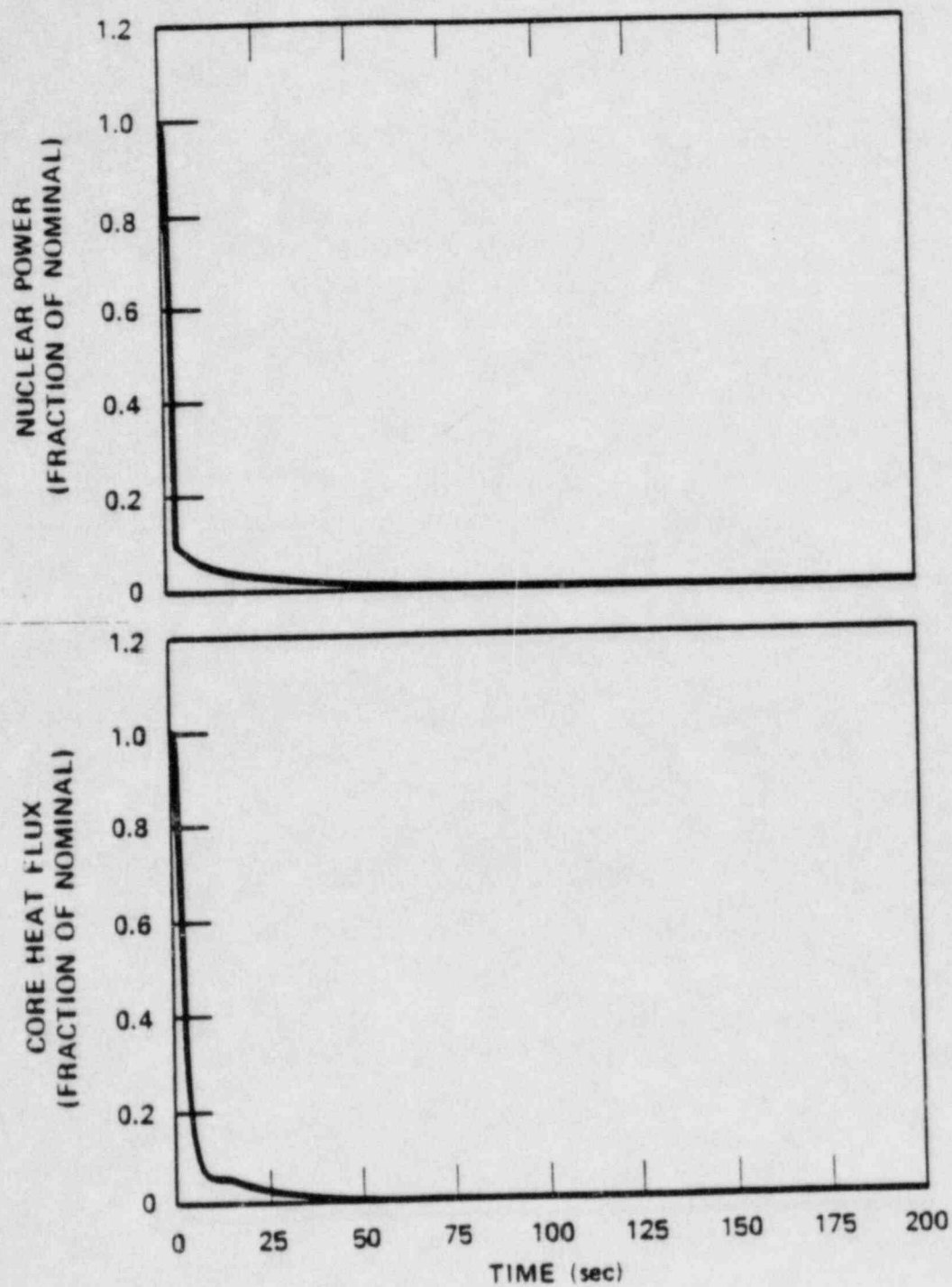


Figure 8. Feedwater Control Malfunction Nuclear Power and Core Heat Flux Versus Time Reactor Trip on Lo-Lo Steam Generator Level (End of Core Life)

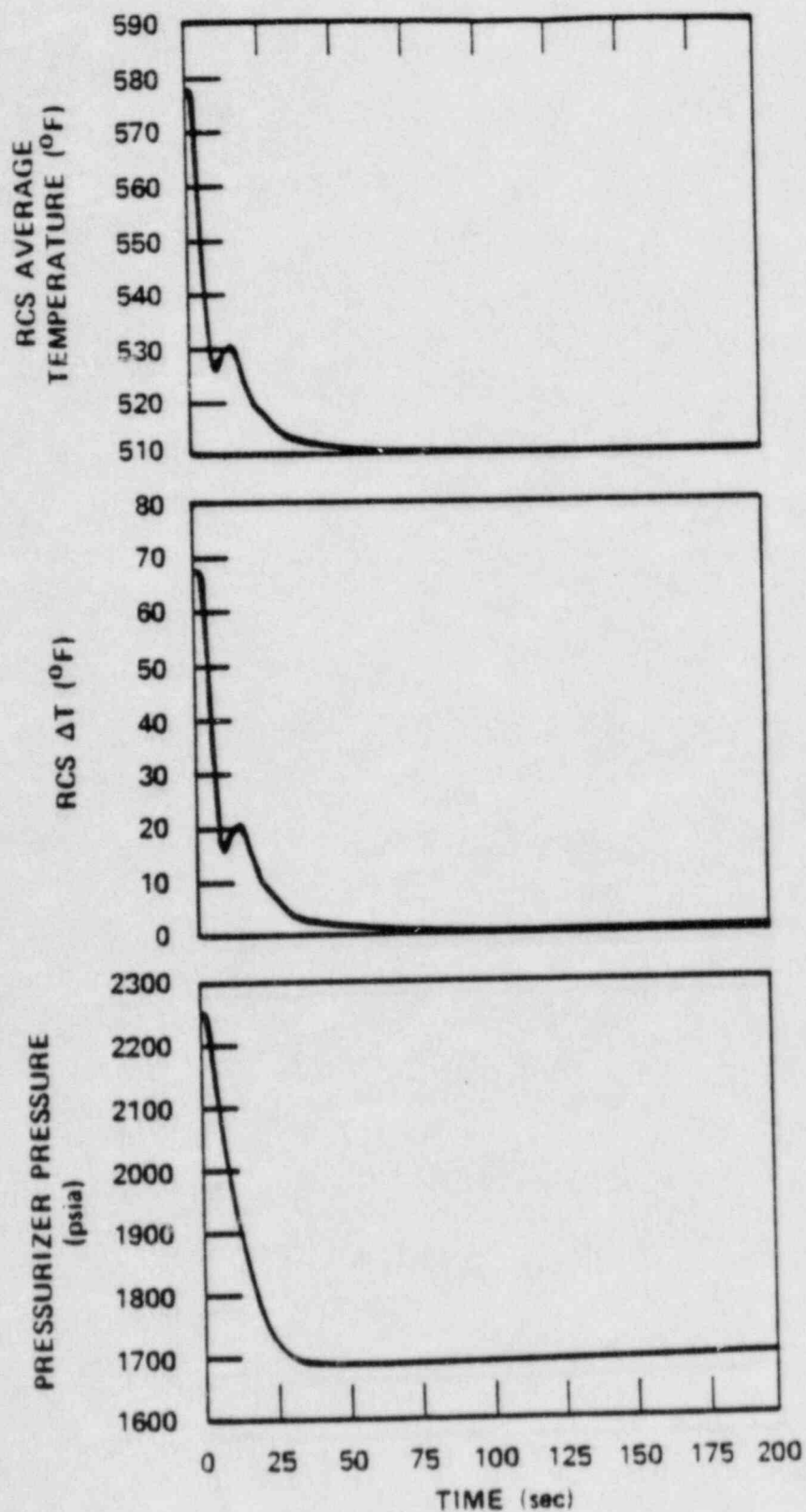


Figure 9. Feedwater Control Malfunction RCS Average Temperature, ΔT and Pressurizer Pressure Versus Time Reactor Trip on Lo-Lo Steam Generator Level (End of Core Life)

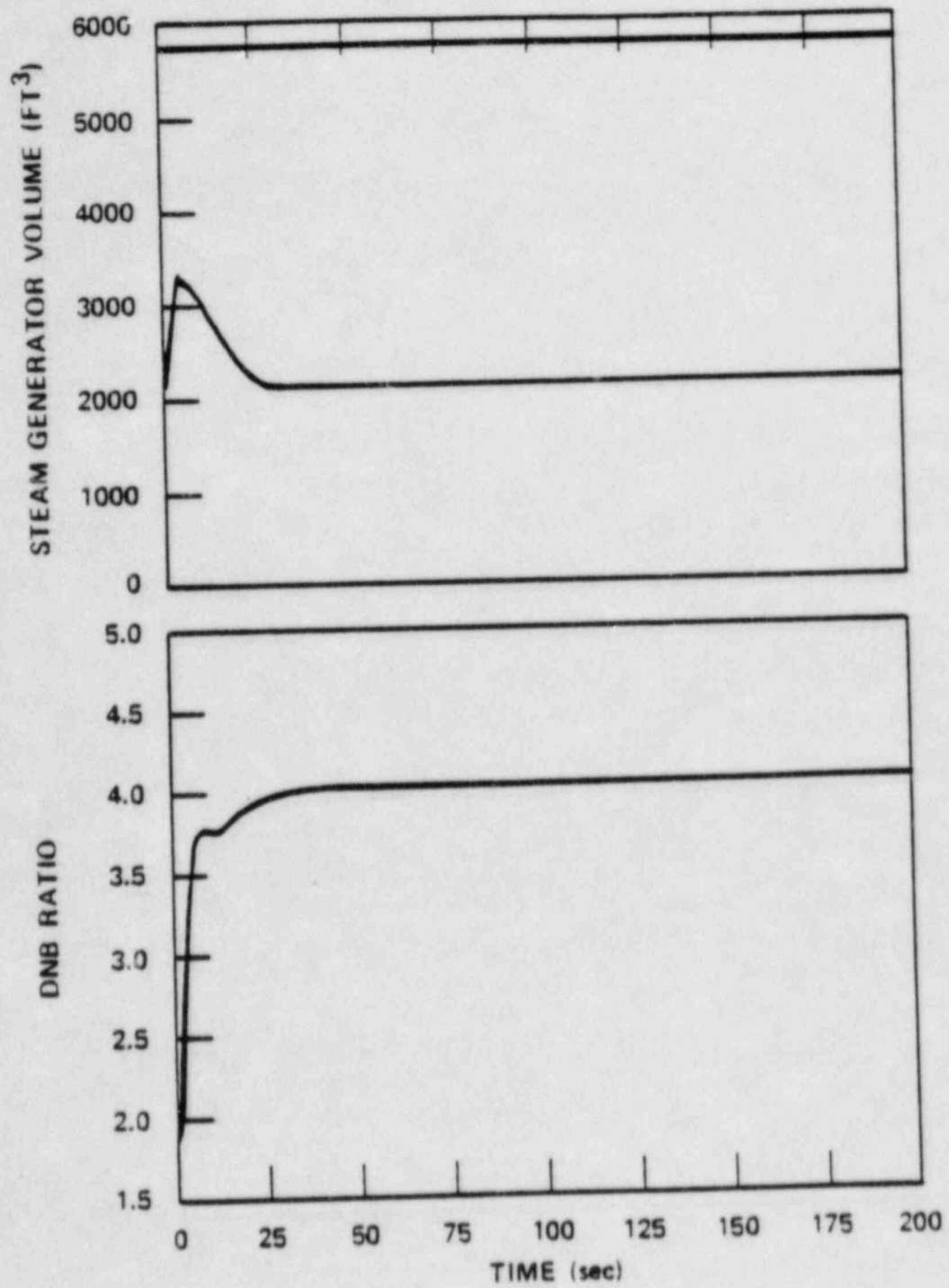


Figure 10. Feedwater Control Malfunction Steam Generator Secondary Side Volume and DNB Ratio Versus Time Reactor Trip on 1 -Lo Steam Generator Level (End of Core Life)

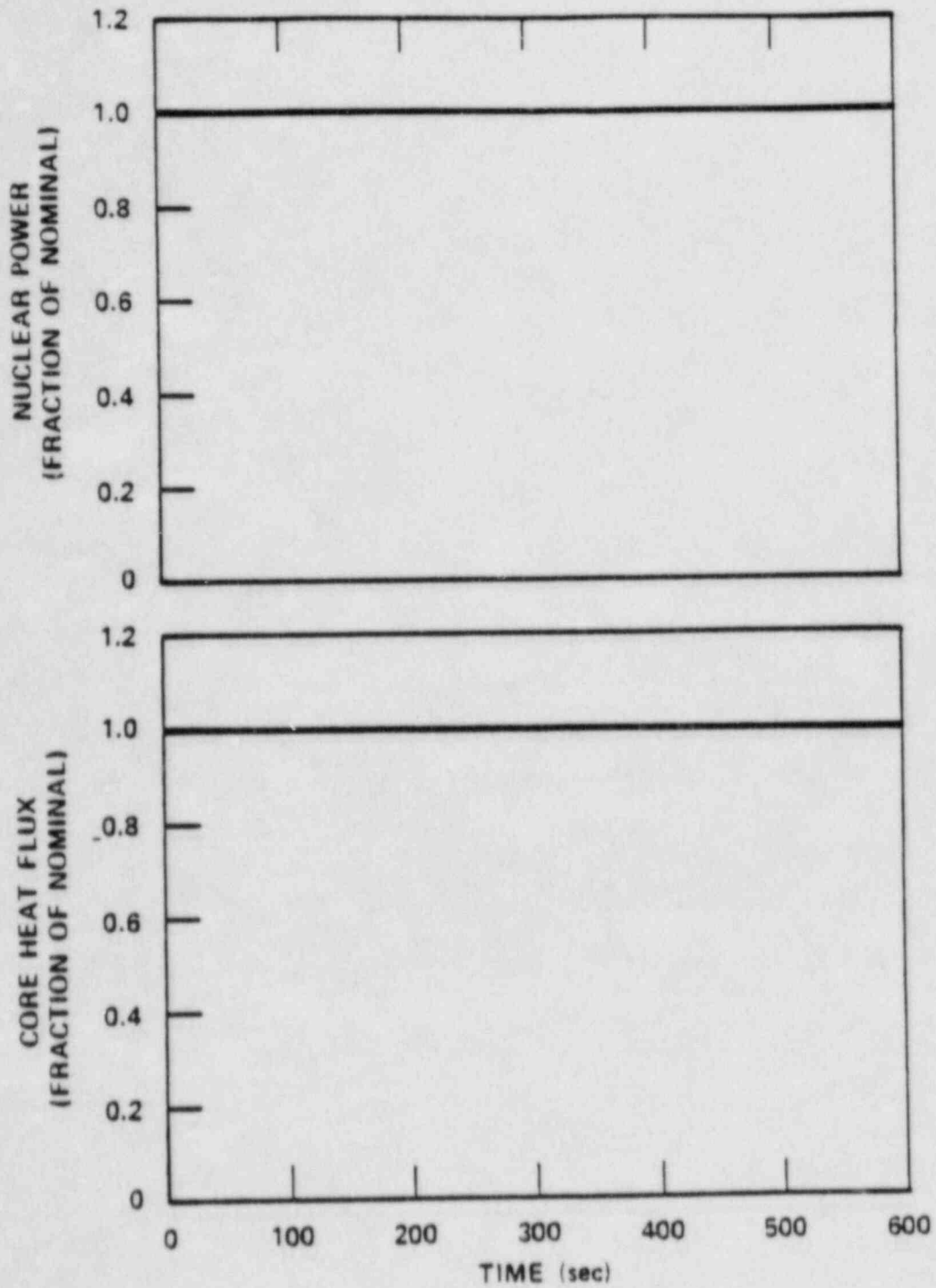


Figure 11. Feedwater Control Malfunction Nuclear Power and Core Heat Flux Versus Time No Reactor Trip (Beginning of Core Life)

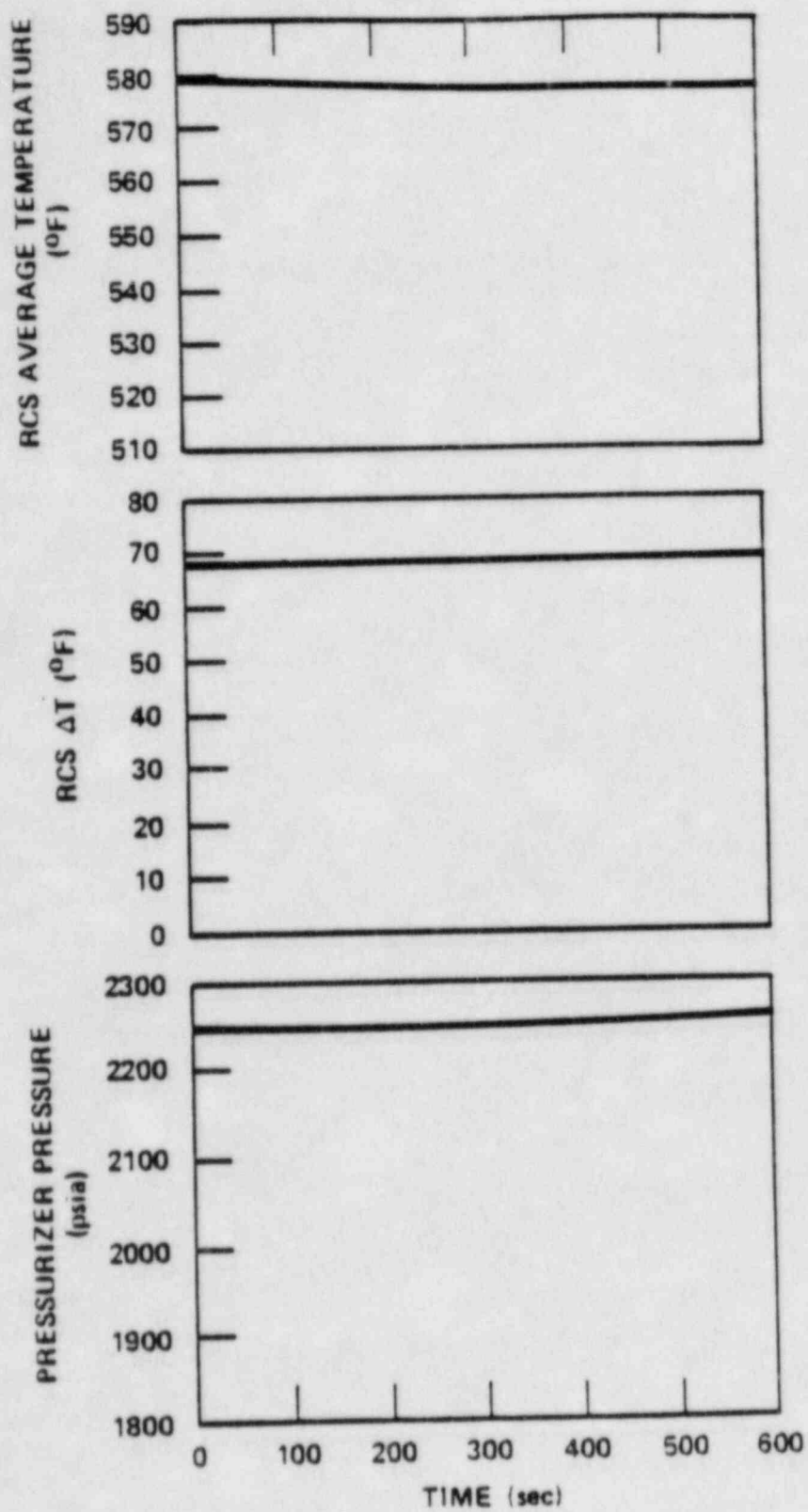


Figure 12. Feedwater Control Malfunction RCS Average Temperature, ΔT and Pressurizer Pressure Versus Time No Reactor Trip (Beginning of Core Life)

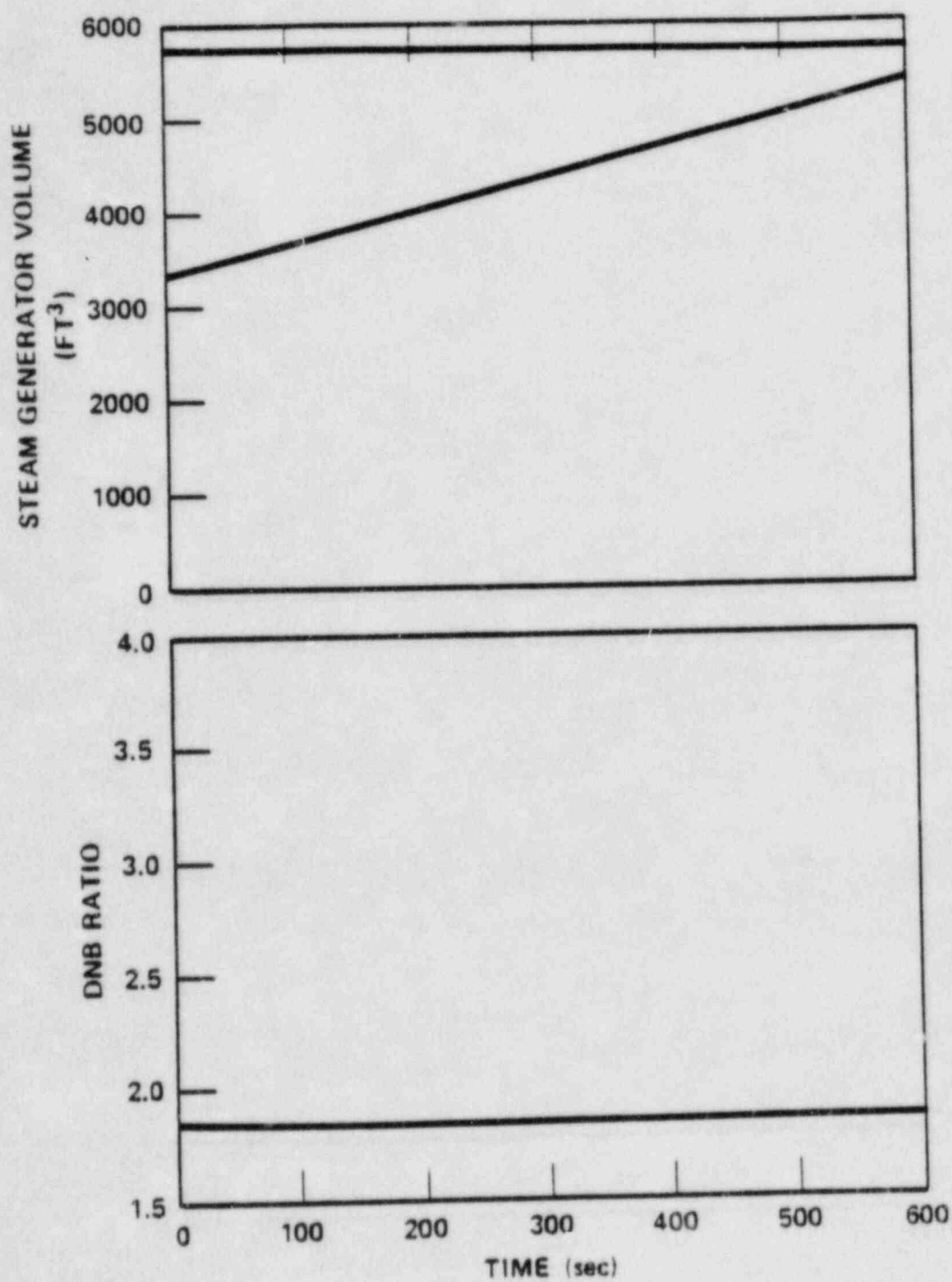


Figure 13. Feedwater Control Malfunction Steam Generator Secondary Side Volume and DNB Ratio Versus Time No Reactor Trip (Beginning of Core Life)

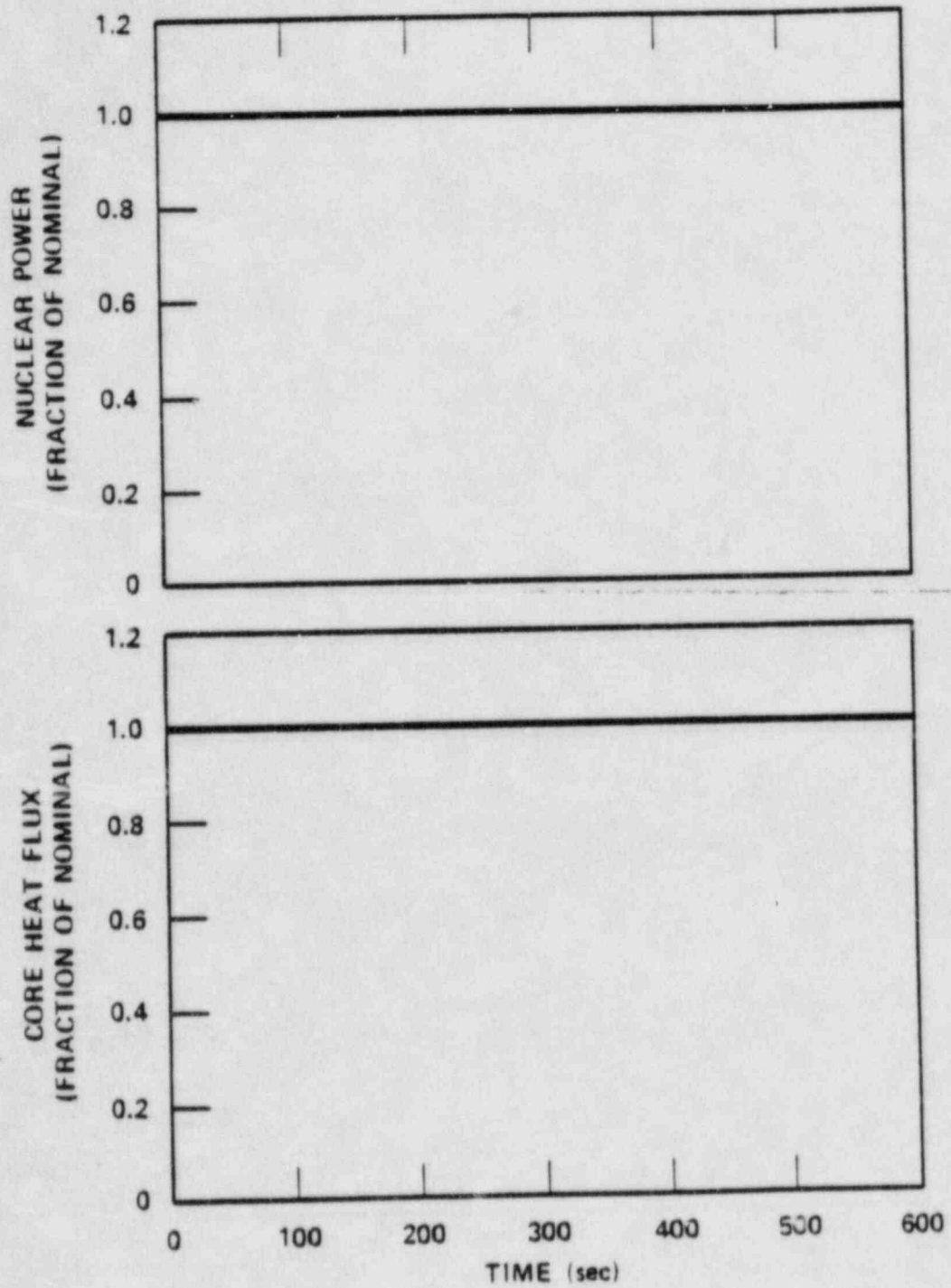


Figure 14. Feedwater Control Malfunction Nuclear Power and Core Heat Flux Versus Time No Reactor Trip (End of Core Life)

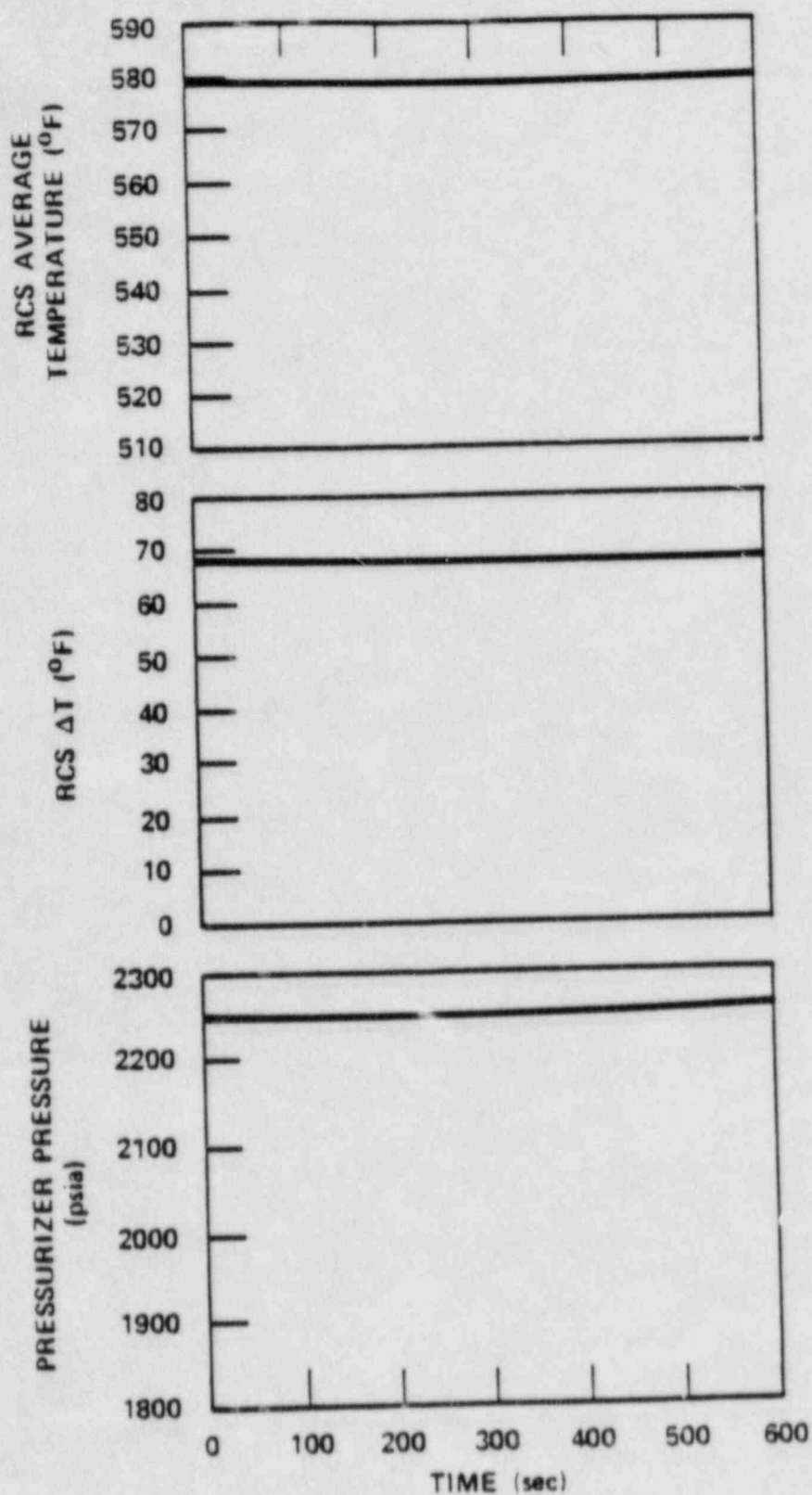


Figure 15. Feedwater Control Malfunction RCS Average Temperature, ΔT and Pressurizer Pressure Versus Time No Reactor Trip (End of Core Life)

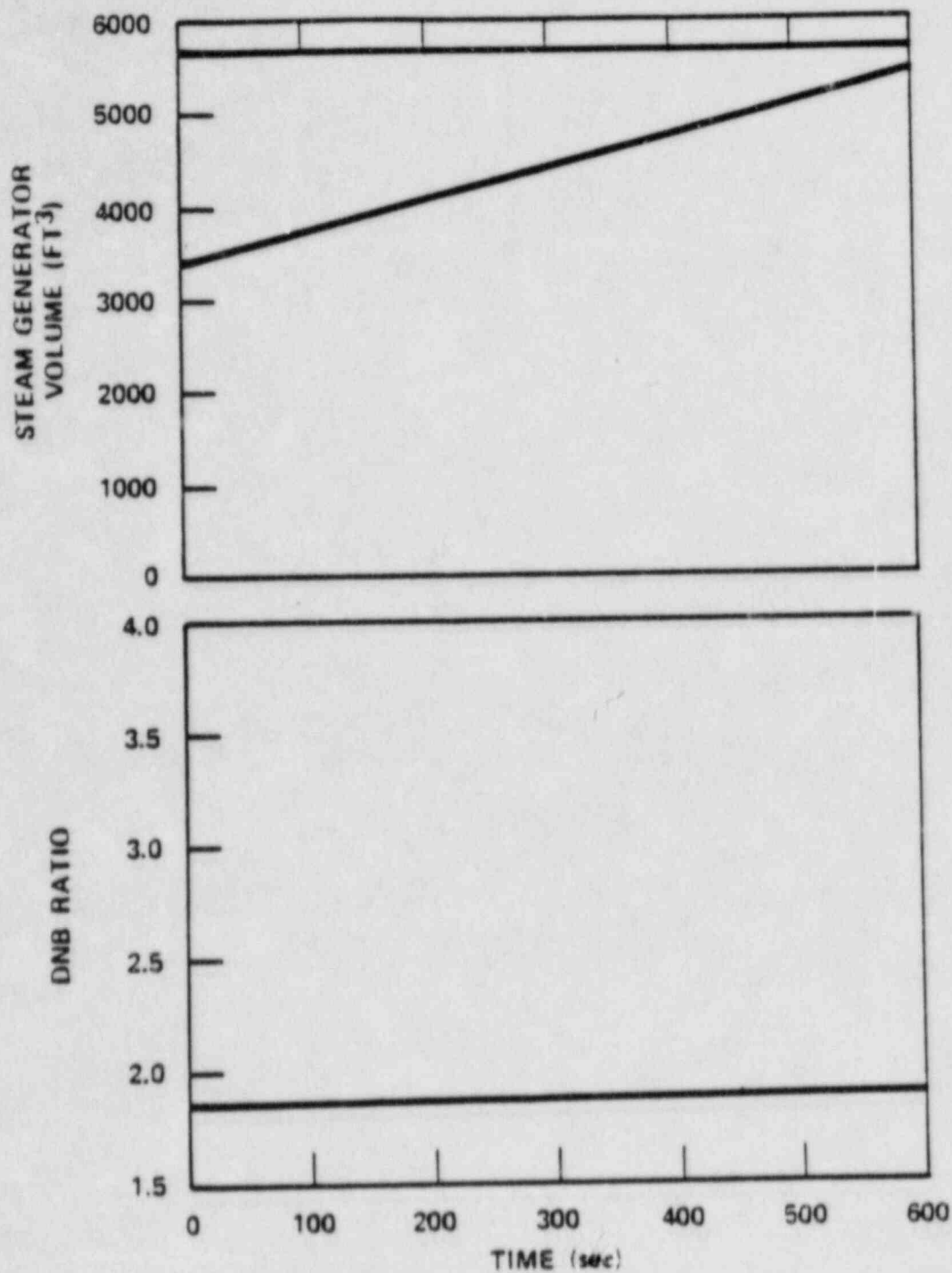


Figure 16. Feedwater Control Malfunction Steam Generator Secondary Side Volume and DNB Ratio Versus Time No Reactor Trip (End of Core Life)

ATTACHMENT 2

Response to ICSB Licensing Position No. 2 on Power Lockout for Motor-Operated Valves

The staff position on this issue states that the Duquesne Light Company (DLC) proposed design modification (adding indicating lights that illuminate when power is available in the normally de-energized circuit) does not meet the single failure criterion of IEEE-STD-279.

DLC has reviewed this issue including the staff's position to add an interlock from "42" to "42a" and "42c" and concluded that IEEE-STD-279 is met by the existing design. Paragraph 4.2 of IEEE-STD-279 states in part, "any single failure within the protection system shall not prevent proper protection action at the system level when required." This criteria is met by the existing design. These valves are a passive safety feature in that an actuation signal is not required to perform their protective action. For example, the cold leg accumulator isolation valves are normally open with the plant operating and the control circuit is locked out via banana plug lockout jacks located on the main control board. Thus, no protective action is required to move the valves to the position required to perform their safety function.

The following features provide assurance the valves remain open during normal operation and that they will be open if required by the safety injection system:

1. Although the valves are normally open, the valves automatically receive an "open" signal upon initiation of safety injection.
2. The valves automatically receive a "block" signal in the "close" circuit upon initiation of safety injection.
3. Redundant valve position indication is provided and available on the main control board (stem mounted limit switches and motor operator limit switches) powered from separate power supplies.
4. An alarm is initiated in the control room when the valve leaves the fully open position and will repeat every 30 minutes if the valve remains open. In addition, a safety injection system-inoperable alarm is provided.
5. The valve position is verified by the operator at least every 12 hours.
6. The valve control circuit has power lockout jacks that are removed when the reactor is at operating pressure in order to prevent inadvertent closure of the valves.