REACTOR PROTECTION SYSTEM DIVERSITY IN WESTINGHOUSE PRESSURIZED WATER REACTORS

April 1969

Author: T. W. T. Burnett

Contributors: J. W. Dorrycott
A. C. Hall
D. H. Risher

APPROVED: J. S. Moore
J. S. Moore, Manager
Core Engineering

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

FOREWORD

Over the past four years, considerable attention has been focused on design criteria and methods of implementation for nuclear power plant protection systems. Of particular difficulty has been the establishment of suitable criteria to deal with the problems of single and multiple failures, channel independence, Control and Protection System independence, and the deviation of Protection System inputs. A key factor in this difficulty has been the conflict between the goal to minimize the number of redundant measurements for any single process variable, with regard to the overall nuclear plant requirements, and the goal to establish a maximum degree of separation between the Protection System and the Control System.

Obtaining an accurate and reliable measurement of a particular process variable is one of the most difficult aspects of an instrumentation system. There are significant problems associated with the physical mounting of the measurement devices including optimum location, supporting structures, access to the equipment for maintenance, and protection against adverse environmental factors. In the case of nuclear power plants, there is also the problem of transmitting the signals from the containment to the control room equipment. All of these factors provide arguments for minimizing the number of separate measurements.

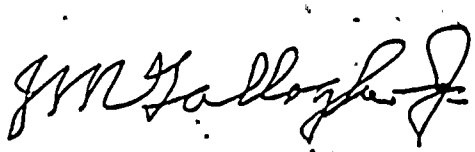
Most of the functions performed by the plant Control System require the same process information as the Protection System. In these cases, Westinghouse provides Control System inputs from Protection System channels. The "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems," IEEE No. 279, permits this design approach, subject to certain restrictions. However, this proposed resolution was not unanimously accepted by members of other United States standards and regulatory agencies, in particular, USASI Sectional Committee N3 (N42), and the AEC-ACRS.

Westinghouse held meetings with members of the AEC to clarify the Westinghouse design approach and to identify the additional design criteria applied by Westinghouse, which go beyond the proposed IEEE criteria. These additional criteria require separation and identification of control and protection equipment and the use of isolation devices to transmit signals from the Protection System to the Control System. It is the position of Westinghouse that these additional criteria offer a resolution to the stated design conflict. Westinghouse has demonstrated by actual implementation of these criteria that a high degree of separation, including proper identification, can be achieved between Protection System equipment and Control System equipment.

More recently, the question of the failure mode changed from that of a single random failure to common-mode failure - a failure mode which would adversely affect all redundant channels of a particular protective function in the Protection System. It is generally recognized that separation of control and protection does not provide defense against the common-mode failures.

The nuclear power plant Control and Protection System design employed by Westinghouse was evaluated in detail with respect to the common-mode failure and presented in a series of meetings to members of the AEC. This report documents the information transmitted in these meetings and provides a technical basis for the development of criteria for design of Protection Systems with adequate consideration for common-mode failures.

The conclusion of Westinghouse based, upon actual experience, previous work, and reinforced by the results presented herein, is that design criteria for nuclear power plant protection systems should permit maximum effective use of process measurements both for control and protection functions including the use of Protection System measurements in the Control System. Such criteria significantly enhance the designer's capability to provide a system with adequate capability to deal with the majority of common-mode failures as well as to provide redundancy for critical control functions.



J. M. Gallagher, Jr.

Consulting Engineer - Control Technology

ABSTRACT

Westinghouse design philosophy for Reactor Protection and Control Systems is to make maximum use, for both protection and control functions, of a wide range of measurements. The Protection and Control Systems are separate and identifiable. The design approach permits not only redundancy of control, providing its own desirable increment to overall plant safety, but also provides a Protection System which continuously monitors numerous system variables by different means; i.e., protection system diversity.

The extent of Protection System diversity has been evaluated for a wide variety of postulated accidents. In most cases, two or more diverse protective functions would terminate an accident before intolerable consequences could occur.

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (Cont'd)

LIST OF FIGURES

LIST OF FIGURES (Cont'd)

1. INTRODUCTION

Westinghouse design philosophy for Reactor Protection and Control Systems is to make maximum use, for both protection and control functions, of a wide range of measurements. This results in a broad spectrum of redundant protection and control functions. The design approach used permits all equipment components to be identified as protection or control and located accordingly, with electrical isolation and physical separation between them. The design approach thus permits not only reduncancy of control, providing a significant and desirable increment to overall plant safety, but also provides a Protection System which continuously monitors numerous system variables by different means; i.e., Protection System diversity.

Although the Protection System design basis requires only that random single failures not negate the Protection System, a considerable depth of protection is achieved by the Westinghouse design approach. Systems designers and reviewers have recently emphasized the importance of achieving a suitable balance of design objectives in regard to functional and equipment diversity, interaction of control and protection functions, testing, and surveillance to achieve a Protection System design that has adequate capability to cope with both random and systematic failure modes. (Systematic failures are also known as common-mode, or nonrandom failures.)

1.1 COMMON-MODE FAILURES AND DIVERSITY

Common-mode, or systematic failures, are those that partially or completely prevent identical instrument channels from performing their function.

Redundancy is not an answer to this type of failure, since all channels are assumed to be affected. Further, these failures cannot be evaluated by probability analysis or reliability data; indeed, they are characterized by oversights or deficiencies which presumably would be corrected when first detected.

The general categories of common-mode failures are:

a) Functional deficiency - The variable being monitored does not provide the information intended during the course of an accident. This deficiency could be caused by the accident's following a different course than calculated by the designers, or by a change in the plant characteristics which changes the relation between the process and the variable being monitored.

b) Maintenance error - This failure includes consistent miscalibration of all channels of a type, and also circuit modification or repair which inadvertently renders the channels functionally inoperative.

c) Design deficiency - Failure of the equipment as installed to meet functional requirements. This could arise through unrecognized dependence on a single, common element, such as ventilation; by an unexpected characteristic (such as saturation or slow response) in all controllers of a type; or by the instrumentation being disabled as a result of the accident.

d) External catastrophe - With proper isolation and separation between redundant channels, this is confined to major disasters such as flood, earthquake, fire, etc. Where separation is not complete, less drastic events can have the same result. For example, a falling object could conceivably sever all cables in a small area.

Considerable effort is being made in Reactor Protection Systems design to prevent these common-mode failures, as illustrated by the examples below. However remote, the possibility of a common-mode failure must nevertheless be considered. The likelihood of maintenance errors can be minimized by proper administrative procedures, identification of Protection System components, and complete documentation of the as-supplied Protection System, including the design basis. Design deficiencies can be largely eliminated by equipment qualification testing and by careful review of all potential common elements.

Redundancy is an accepted defense against random failures which affect only one component or channel at a time. Similarly, diversity is a defense against common-mode failures which could affect multiple channels.

Such protective diversity can be achieved in either of two ways: equipment diversity, by providing different types of instrumentation to monitor the same variable, or functional diversity, by monitoring different plant variables. Functional diversity entails some degree of equipment diversity, primarily with respect to sensors and setpoints. More importantly, however, functional diversity is not dependent on the calculated response of any one variable during an accident. As a converse of this, functional diversity is more complex to demonstrate since the response of several variables must be analyzed for each type of accident evaluated.

The Westinghouse Protection System is therefore evaluated in this report with respect to functional diversity. To demonstrate diversity where protective action is needed, it is necessary to show combinations of two or more of the

following "barriers" for each accident. Some of these are addressed to the probable need for protective action, rather than to the Instrumentation System itself. This is considered a reasonable approach to judging the adequacy of a Protection System.

a) Tolerable consequences for expected conditions - Although "worst case" analysis might fail to prove that protection is not needed, the vast majority of cases may have acceptable consequences. Whether or not this is a suitable barrier depends on the probability of adverse conditions (such as excessive inserted rod worth) and the design and operating precautions taken to prevent them.

b) Low probability of accident - Probability of the initiating fault might be considered, but only in conjunction with the probable consequences. That is, a loss-of-coolant accident does not require less protection than a loss of flow accident simply because it is less likely to occur.

c) Control interlocks - Rod stops or other devices which arrest or modify spurious control action short of reactor trip can be part of the Protection System. Protection System design standards, equipment testing, and Technical Specification limits would therefore be applied.

d) Manual action - Manual action can be considered a reliable backup to automatic protection, depending on the accident rate, the complexity of the problem and corrective action, and the alarms and indication provided.

e) Automatic reactor trip - Each accident may have a "principle" reactor trip associated with it.

f) Backup reactor trip - A second reactor trip function, of a diverse type, is an additional barrier.

In all but a few cases in the Westinghouse design, a specific reactor trip is not categorically either "principle" or "backup": it serves as the principle protection against some accidents, and as backup protection against others.

1.2 PROTECTION SYSTEM EVALUATION

An accident-by-accident evaluation has been performed in order to evaluate the "depth" or degree of diversity provided by current Westinghouse design. As expected, diversity could not be demonstrated for all accidents. The results in general, however, indicate a considerable degree of Protection System diversity.

The evaluation, reported in Section 5 of this report, analyzed each postulated accident without credit for protective action to the point at which one of the three following events occurs:

a) Inherent plant characteristics terminated the accident;

b) The consequences are clearly intolerable; or

c) Existing analytical methods are no longer valid (for example, system calculations cannot be performed with any degree of confidence if severe core damage occurs).

In this type of evaluation, the amount of analytical rigor must be reduced as conditions become increasingly remote and safety limits are exceeded. This is because present technology cannot rigorously support assumptions as to system behavior for these remote cases. In large part, this fact explains the reason why such conservative safety limits are selected for design purposes.

2. SUMMARY

In the Westinghouse Reactor Control and Protection Systems, the Control System is separate and distinct from the Protection System. Although the Protection System is independent of the Control System, the Control System is highly dependent upon signals derived from the Protection System through isolation amplifiers. This interrelationship is illustrated in Figure 2-1. The design of the Control and Protection Systems and the interactions between them are discussed in detail in Sections 3 and 4 of this report.

The design philosophy is to make maximum usage, for both control and protection purposes, of all measurements of plant variables. For each variable monitored, the best type of equipment available is selected as the vehicle of measurement. Clearly, the requirements for measurements for control or protection purposes so nearly overlap that the optimum equipment for one purpose is also the optimum for the other.

It is recognized by those responsible for Protection System design and review that little if any additional safety is achieved by utilizing independent, but identical, measurements for control and protection. In fact, it is Westinghouse's position that additional identical channels are seriously disadvantageous in that more penetrations, maintenance, and control room readouts are required. For example, operator surveillance of protection channels is necessarily diluted when plant operation is dependent on other indications.

In a large pressurized water reactor plant, it is almost axiomatic that any perturbation which encroaches on safety limits significantly affects many variables. For example, a reactivity excursion - such as accidental rod withdrawal - causes not only an increase in neutron flux and core power, but also an increase in coolant temperatures and in pressurizer pressure and level.

Reliable control is obviously the best approach to plant safety. The prime purpose of a control system is to limit excursions before protective action is necessary. Since the control devices must be capable of limiting excursions, they are also capable of causing an excursion - perhaps in the opposite direction - if spuriously actuated. Failure of the Control System, either by not acting when needed, or acting when not needed, decreases the level of safety. Redundancy of control, where applicable, is therefore highly desirable.

Pressurizer pressure control is a prime example of efficient use of redundant measurements for safe operation via a reliable Control System. Two power-operated pneumatic relief valves are provided to limit pressure excursions within the normal operating range. Although not essential to safety, these valves increase safety margins for system overpressure (overpressure protection is provided by the high pressure reactor trip and safety valves). Should either valve be actuated spuriously, however, protection against the reduction in pressure might also be required.

four pressure control channels, derived form the four pressure protection channels, are used to insure that no single instrument failure can prevent relief when needed, nor can any single instrument failure cause either valve to reduce pressure to the point at which protection would be needed. Two pressure channels are used to control each valve. One pressure channel serves as an interlock, blocking the air supply to the valve on a low pressure alarm. Since the pneumatic valve requires air to open, this low pressure alarm closes the valve (if open) and holds it closed. In the absence of a low pressure alarm on the first channel, a high pressure alarm on the second channel opens the valve.

From the Protection System viewpoint, the corollary to maximum usage of all measurements is that protection against any given accident is not necessarily confined to measurement of just one variable. Thus the reactivity excursion noted previously, the reactor trip on high pressurizer water level, also provides a degree of protection, even though the basic purpose of this trip is to protect the pressurizer relief piping from water relief surge through the safety valves. Since completely different types of measurement are used for neutron flux and pressurizer water level, diversity does exist in the Protection System.

The extent of such diversity is evaluated in Section 5 for a wide variety of accidents. In most cases, two or more diverse reactor trips terminate an accident before catastrophic consequences can occur. However, the second trip reached (the "backup") generally does not prevent the design safey limit from being exceeded. In this context, the design safety

limit, such as a DNB ratio of 1.30, is itself a highly conservative limit: exceeding this limit does not imply intolerable consequences.

In one case evaluated - the hypothetical rod ejection accident - protection system diversity could not be adequately demonstrated for the worst case. However, a rod ejection is considered to be an extremely unlikely accident - one caused by complete and instantaneous mechanical failure of a control rod pressure housing. Further, the probable consequences, as distinct from the worst case, are tolerable since most control rods are fully withdrawn from the core. Even those rods that remain inserted are seldom inserted to their insertion limits.

For another type of accident - complete loss of feedwater - diversity of reactor trips does exist. However, automatic actuation of the auxiliary feedwater system is not diverse for all of the ways in which feedwater flow could be lost. For those cases, it is shown that manual actuation constitutes a reliable back-up to automatic actuation.

ILLUSTRATION OF CONTROL
AND PROTECTION DESIGN

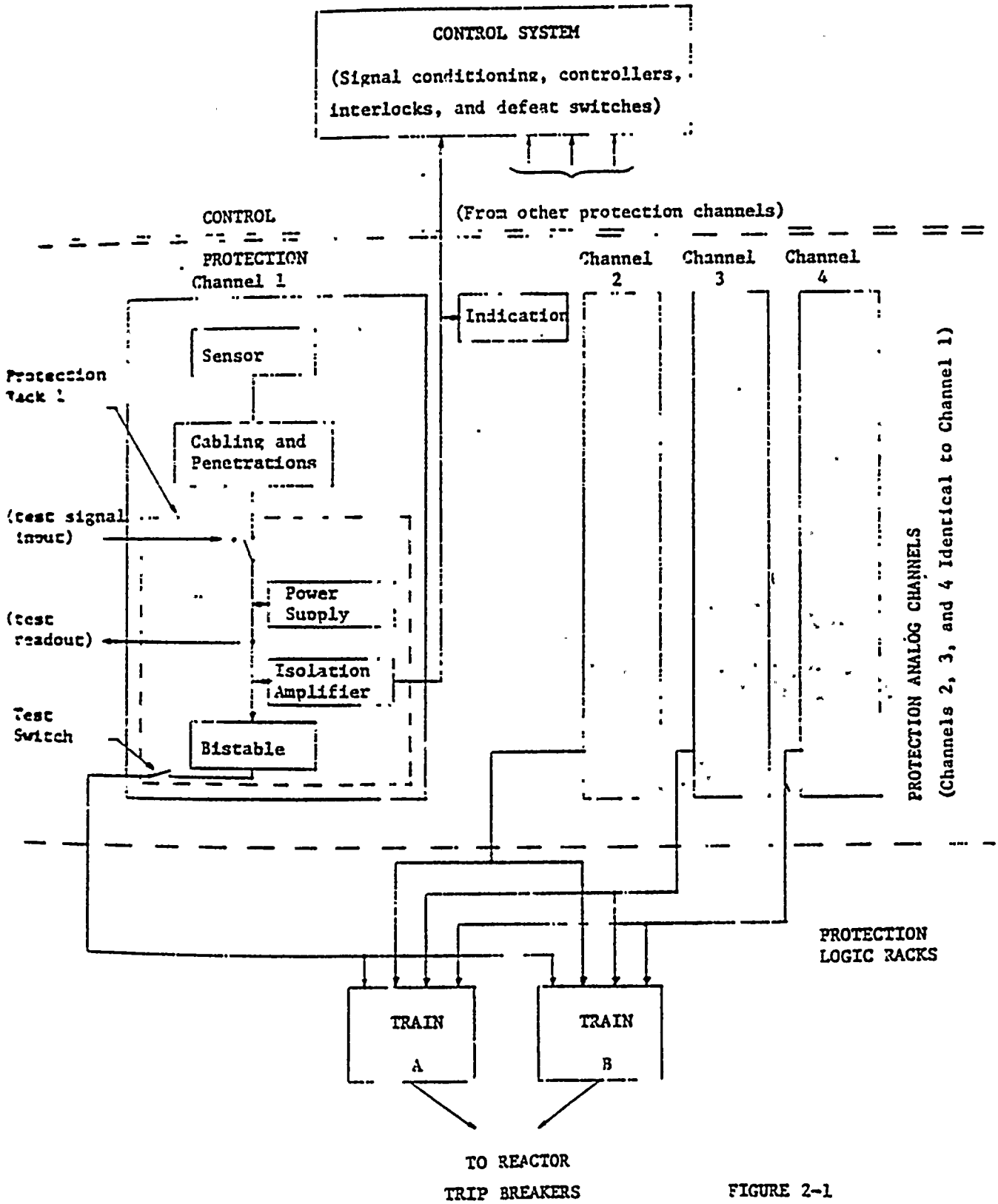


FIGURE 2-1

3. FUNCTIONAL DESCRIPTION, REACTOR CONTROL AND PROTECTION SYSTEM

3.1 REACTOR PROTECTION SYSTEM

3.1.1 GENERAL

The following Reactor Control and Protection System functional description is based on the Robert Emmett Ginna Nuclear Station of the Rochester Gas and Electric Co. (RG&E). It is representative of Westinghouse design practice.

All reactor trips meet the following criteria:

a) A single failure shall not negate a reactor trip

b) All channels are capable of calibration and maintenance at power.

3.1.2 REACTOR TRIPS

A resume of reactor trips, means of actuation and coincident circuit requirements is given in Table 3.1-1.

Manual Trip

Depressing either of two manual push buttons on the main control board actuates a reactor trip.

High Nuclear Power (Power Range)

Dual trip settings are provided:

a) Low (approximately 25%)

b) High (approximately 110%).

The low setting can be manually blocked when power increases above P-10* (approximately 10% power) and is automatically reinstated when power decreases below P-10.

These circuits trip the reactor when two of the four external ion chamber average flux signals are above the trip setpoint.

High Nuclear Power (Intermediate Range)

This circuit trips the reactor when either of the two intermediate channels indicate above the trip setpoint. It may be manually blocked when power is above P-10 and is automatically reset when power decreases below P-10. Expected trip setpoint is 25%.

High Nuclear Power (Source Range)

This circuit trips the reactor when either of the two intermediate range channels indicate above the trip setpoint. It may be manually blocked when two intermediate range channels reads a value above P-6 and is automatically reinstated when both intermediate range channels decrease below P-6. Trip setting is between P-6 and the maximum source range power level.

---

* P-( ) designates a permissive circuit to block or activate a trip function. These circuits are defined in Section 3.1.3.

Overtemperature ΔT Trip

The purpose of this trip is to protect the core against DNB for any combination of power, pressure, temperature, and axial core power distribution. Two-out-of-four trip logic is used, with two channels per reactor coolant loop. For each channel, the indicated ΔT is used as a relative measure of reactor power and is compared with a continuously calculated setpoint of the form:

$$\Delta T_{setpoint} = K_1 + K_2 \times \text{Pressure} - K_3 \times T_{avg} - f(\Delta I)$$

When the reactor coolant loop ΔT exceeds the calculated setpoint, the affected channel is tripped.

In the above equation, ΔI is the difference between the top and bottom power-range ion chamber signals. This compensation signal automatically reduces the trip setpoint if adverse axial core power distribution exists. Dynamic compensation of the T_{avg} signal is also provided to compensate for instrument and piping delays between the reactor core and the loop temperature sensors.

A schematic representation of this circuit is shown on Figure 3.1-1. An illustration of the setpoint is shown on Figure 5.1-6.

Overpower ΔT Trip

The purpose of this trip is to protect against excessive power (fuel rod power density). Two-out-of-four trip logic is used; there are two channels per reactor coolant loop.

The setpoint for each channel is calculated as:

$$\Delta T_{setpoint} = K_4 - K_5 \frac{d}{dt} T_{avg} - K_6 (T_{avg} - T^{\circ}_{avg}) - f(\Delta I)$$

In this equation, $f(\Delta I)$ is the same function as used in the overtemperature ΔT setpoint equation. The term K_5 compensates for the piping and instrument time delay. The term K_6 compensates for the change in density and heat capacity of water with temperature (T°_{avg} is the nominal T_{avg} at full power). Both K_5 and K_6 are limited such that the rate and/or magnitude of T_{avg} can only decrease the ΔT trip setpoint from its normal value at full power. Expected steady-state trip setpoint is 110% of the indicated ΔT at full power; i.e., 110% power.

A schematic representation of this cricuit is shown on Figure 3.1-2.

Low Pressure Trip

The purpose of this trip is to protect against excessive boiling in the core and to limit the pressure range in which core DNB protection is required for the overtemperature ΔT reactor trip. This circuit trips the reactor on coincidence of two-of-four channels. It is automatically blocked below P-7. The expected setpoint is 1715 psig.

High Pressure Trip

The purpose of this trip is to protect against overpressure and to limit the pressure range in which core DNB protection is required of the overtemperature ΔT trip. Expected setpoint is 2385 psig.

This circuit trips the reactor on coincidence of two-of-three channels.

High Pressurizer Water Level Trip

This trip provides a backup to the high pressure trip and also prevents the pressurizer safety and relief valves from relieving water for credible accident conditions. Expected setpoint is 92% of span.

This circuit trips the reactor on coincidence of two-of-three channels. It is automatically blocked below P-7.

Low Reactor Coolant Flow

This circuit is provided to protect the core from DNB following a loss of coolant flow accident. The means of sensing a loss of coolant flow accident are as follows:

a) Measured low flow in the reactor coolant piping

b) Reactor coolant pump circuit breaker open

c) Undervoltage on reactor coolant pump bus

d) Underfrequency on reactor coolant pump bus

The low flow trip signal is actuated by the coincidence of two-of-three signals per loop. Above P-7, reactor trip occurs for a loss of flow in both loops; above P-8, reactor trip occurs for a loss of flow in either loop. Expected setpoint is 90% of indicated full flow.

The reactor trip signal derived from reactor coolant pump breaker position is actuated by a single auxiliary contact for each reactor coolant pump breaker. Trip logic is similar to the low flow trip; above P-7 reactor trip occurs for a "breaker open" signal from any two breakers; above P-8, a signal from any one breaker actuates a reactor trip.

An undervoltage reactor trip provides additonal reactor protection against a complete loss of flow accident caused by loss of power. A reactor trip occurs on low voltage on both reactor coolant pump buses, as sensed by either of two undervoltage sensors on each bus. Expected setpoint is 70% of normal voltage.

In principle, a rapid decrease in electrical frequency can decelerate the reactor coolant pumps faster than a complete loss of power. An underfrequency condition on both reactor coolant buses, as sensed by either of two underfrequency relays on each bus, trips the reactor and opens both reactor coolant pump circuit breakers. Expected setpoint is approximately 58 cps.

Safety Injection System Actuation Trip (SIS)

Upon actuation of the Safety Injection System, the reactor is tripped to decrease the severity of the accident condition. The means of actuating the Safety Injection System and thus tripping the reactor are as follows:

a) Low pressurizer pressure (1715 psig) in coincidence with low pressurizer water level (5% span). Any one of the three circuits actuates the SIS. This function may be manually bypassed below 2000 psig.

b) Low Pressure (500 psig) in any steam line. A coincidence of two-of-three signals for any steam line actuates this function. This function can be manually bypassed when reactor coolant pressure is below 2000 psig.

c) High containment pressure (6 psig). A coincidence of two-of-three signals actuates the SIS.

d) Manual Actuation.

Turbine Trip

A turbine trip, sensed by loss of autostop oil pressure or by turbine stop valve closure, actuates a reactor trip during high power operation. Trip logic is two-or-three for the autostop oil pressure switches and two-of-two for the stop valve position switches. This trip is in coincidence with permissive circuit P-7 (blocked below 10% power) and permissive circuit P-9 (blocked below 50% power unless condenser steam dump is blocked).

Low Feedwater Flow Reactor Trip

For either steam generator, low feedwater flow (compared to steam flow) in coincidence with low steam generator water level actuates a reactor trip. This protects the reactor against a sudden loss of heat sink. This condition is sensed for either steam generator if either of two steam flow and feedwater flow channels indicate a difference greater than a setpoint and either of two steam generator narrow-range level channels indicate less than a setpoint. Expected setpoints are 0.7×10^6 lbs/hr and 30% of span respectively.

Low Steam Generator Water Level Trip

The purpose of this trip is to protect the reactor from a loss of heat sink for the case of a sustained steam/feedwater flow mismatch which is too small to actuate the low feedwater flow trip.

This trip is actuated on coincidence of two-of-three low-low level signals in any steam generator. Expected setpoint is 15% of narrow range level span.

3.1.3 PERMISSIVE CIRCUITS

Reference has been made previously to permissive circuits. The permissive circuits are used to block certain activities as well as to permit other activities.

List of Permissive Circuits

Number	Function	Input
1	Rod withdrawal stop on overpower (Automatic and manual)	One-of-four high nuclear power (power range)*; one-of-two high nuclear power (intermediate range*†; one-of-four overtemperature ΔT*; or one-of-four overpower ΔT*.
2	Automatic rod withdrawal stop at low power.	One-of-one turbine first stage steam pressure
3	Automatic rod withdrawal stop on rod drop	One-of-four rapid decrease of nuclear power or rod bottom indication
5	Selection of steam dump controller mode	Turbine trip signal
6	Permit manual block of source range high nuclear power trip	One-of-two high intermediate range nuclear power allows manual block, two-of-two low intermediate range nuclear power automatically reinstates trip.

* Manual bypass on individual channels.
† May be manually blocked if permissive circuit P-10 is cleared.

List of Permissive Circuits (Cont'd)

Number	Function	Input
7	Permissive power (block various trips at low power)	Three-of-four low nuclear power and one-of-two low turbine impulse stage pressure
8	Block single primary loop loss of flow trip	Three-of-four low nuclear power
9	Block reactor trip on turbine trip	Three-of-four low nuclear power and condenser steam dump available (not locked out by high condenser pressure or by loss of both circulating water pumps)
10	Permit manual block of intermediate range power level trip and rod stop and low power range trip	Two-of-four high nuclear power allows manual block, three-of-four low nuclear power automatically reinstates the trips

3.1.4 ROD STOPS

A complete list of rod stops is noted below.

Rod Stop List

Function	Actuation Signal	Rod Motion to be Blocked
a) Rod drop	One-of-four rapid power range nuclear power decrease or any rod bottom signal	Automatic withdrawal (redundant contacts)
b) Nuclear Overpower	One-of-four high power range nuclear power or one-of-two high intermediate range nuclear power	Automatic and manual withdrawal

Rod Stop List (Cont'd)

Function	Actuation Signal	Rod Motion to be Blocked
c) High ΔT	One-of-four overpower ΔT or one-of-four overtemperature ΔT (Manual bypass on individual ΔT channels)	Automatic and manual withdrawal

(Actuation of this rod stop initiates a continuous turbine load reduction until the actuation signal is removed).

d) Low power	One-of-one low turbine impulse stage pressure	Automatic withdrawal
e) T_{avg} deviation	One-of-four T_{avg} deviation from average T_{avg}	Automatic withdrawal and insertion

3.1.5 INDICATION

Control Board Indicators and Recorder

All transmitted analog signals which actuate reactor trips, rod stops, or permissive circuits are either indicated or recorded for every channel. Also, variable trip setpoints (overpower ΔT and overtemperature ΔT) are indicated or recorded for every channel.

Central Board Annunciator Panel

Any of the following conditions actuate an alarm:

a) Reactor trip (first out annunciator)
b) Partial reactor trip (any channel)
c) Major deviation of any control variable (pressure, T_{avg}, pressurizer level, nuclear power, and steam generator level) for any channel.

Control Board Status Panel

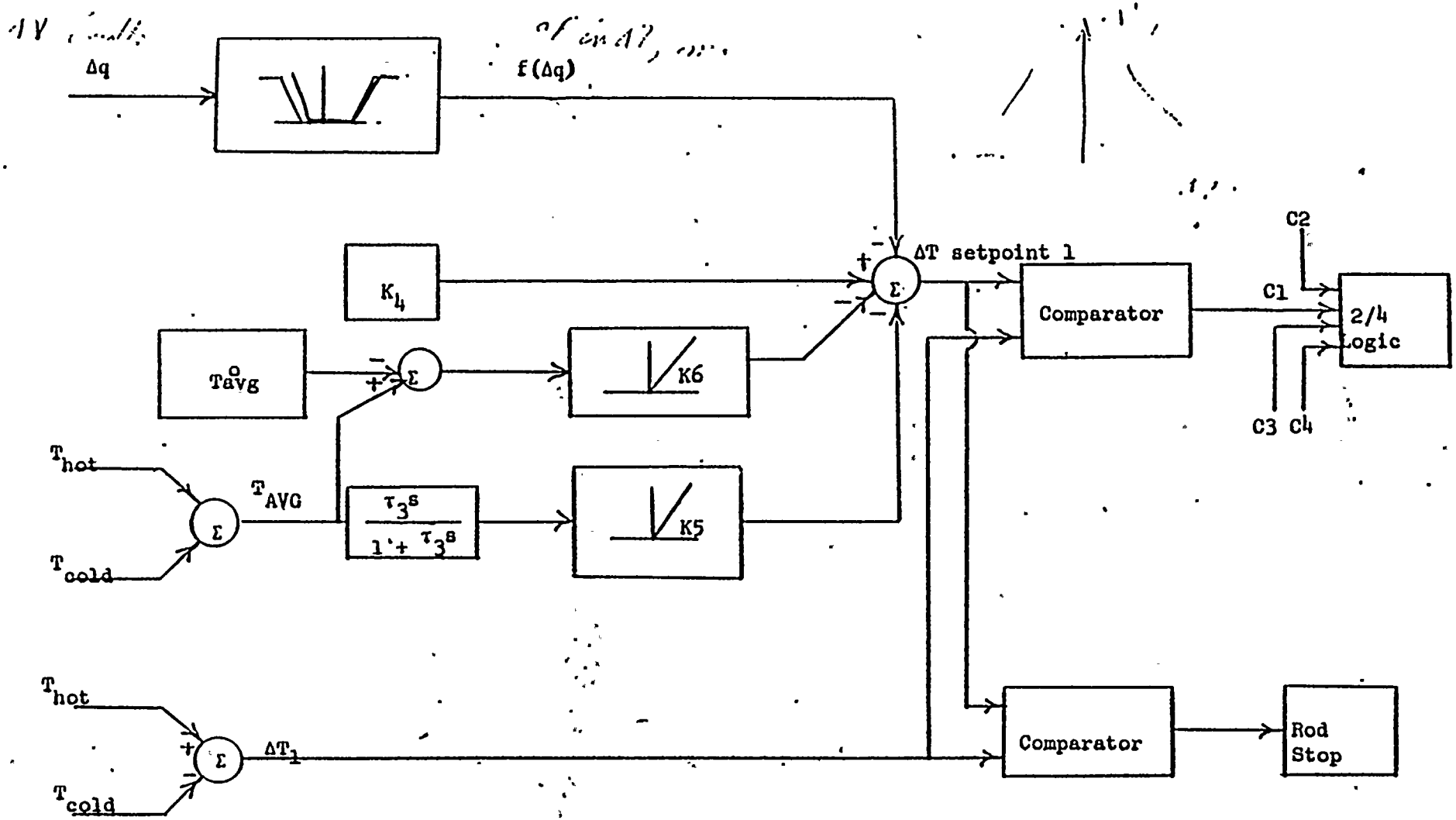
a) The status of each reactor trip channel is continuously displayed on the trip status panel.

b) The status of each permissive circuit is continuously displayed on the permissive status panel.

c) Each reactor trip channel bypass is continuously indicated on the bypass status panel.

TABLE 3.1-1
REACTOR TRIP LIST

	TRIP	COINCIDENCE CIRCUITRY & INTERLOCKS	COMMENTS
1.	Manual	1/2, no interlocks	
2.	High nuclear flux	2/4, no interlocks for high setting P-10 for low setting	High and low settings; manual block and automatic reset of low setting
3.	High nuclear flux (intermediate range)	1/2, P-10	
4.	High nuclear flux (source range)	1/2, P-6	
5.	Overtemperature ΔT	2/4, no interlocks	
6.	Overpower ΔT	2/4, no interlocks	
7.	Low pressure	2/4, blocked by P-7	
8.	High pressure	2/3, no interlocks	
9.	High pressurizer water level	2/3, blocked by P-7	
10a.	Low Flow	2/3 per loop, p-7, P-8	
10b.	Pump breaker trip	1/1 per loop, P-7, P-8	
10c.	Undervoltage	1/2 + 1/2, P-7	
10d.	Underfrequency	1/2 + 1/2, P-7	
11.	SIS actuation	1/3, (low pressurizer pressure and low pressurizer level); 2/3 Low pressure in any steam line; or 2/3 high containment pressure	
12.	Turbine trip	2/3 autostop oil or 2/2 stop valves, P-7, P-9	
13.	Low feedwater flow	1/2 + 1/2 per loop, (flow mismatch in coincidence with low level)	
14.	Low-low S.G. water level	2/3, per loop	



OVERPOWER ΔT CHANNEL

(ONE CHANNEL OF FOUR SHOWN)
FIGURE 3.1-2

3.2 STEAM DUMP CONTROL SYSTEM

Two types of steam dump are available: condenser dump and atmospheric relief.

The steam cycle valve arrangement is shown on Figure 3.2-1.

3.2.1 CONDENSER STEAM DUMP SYSTEM

System Design

Steam lines are installed to dump steam from the steam generators directly to the condenser, bypassing the turbine. Connections with the steam mains are downstream of the steam main isolation valves. Dump valves and lines are sized to pass 35% of turbine maximum calculated steam flow at full load steam pressure.

Condenser steam dump performs three functions:

a) Following a sudden loss of load of up to 210 MWe (about 45% of maximum calculated turbine load), condenser dump acts as an artificial load removing excess power and stored energy while the reactor power is decreased to match the reduced turbine load. In this manner, the condenser steam dump acts to prevent a reactor trip.

b) Condenser steam dump, together with feedwater addition, removes stored energy in the Reactor Coolant System following a plant trip, bringing the plant to equilibrium no load condition without

actuation of the steam generator safety valves. It also maintains the plant at hot shutdown by removing residual heat.

c) Condenser steam dump is used for plant cooldown to cold shutdown.

Condenser steam dump is used to improve operational flexibility. For example, a plant trip may occur following a large load reduction if condenser steam dump is not available.

The condenser steam dump system uses modulating, linear-characteristics, air-operated valves (air to open). Their stroke time is approximately 5 seconds. In addition, they can be tripped from the full closed to the full open position within 3 seconds after receiving an input electric trip signal. While this trip signal exists, the valves are held in the fully open position. When the trip signal does not exist, the valve position is determined by a variable input electrical signal.

For condenser protection, condenser steam dump is blocked by high condenser pressure. Other interlocks (described below) are used in the same manner to avoid spurious operation.

Spurious actuation of steam dump may cause a plant trip. In addition, if the valves stay open, an uncontrolled cooldown results. For these reasons, the steam dump control system is required to meet the criterion that no signal failure shall cause spurious actuation.

Control System

The functional block diagram for the Condenser Steam Dump Control System is shown on Figure 3.2-2.

Load Rejection Control

For partial loss of turbine load, steam dump is controlled by the error signal between T_{avg} and T_{ref}, where T_{avg} is the average of four reactor coolant average temperatures and T_{ref} is the programmed set-point for T_{avg} as a function of turbine load. (These signals are the same as those used in the Reactor Control System.) Following a turbine load decrease, T_{ref} is immediately reset to a lower value, causing an error signal. If the error signal exceeds the deadband for the load rejection controller, the dump valves are modulated open. If the error signal exceeds the HI setpoint, a trip signal is generated which rapidly opens four of the eight valves to their fully-open position. At the occurrence of a HI-HI trip signal, all eight valves trip open.

The distinction between modulating and tripping valves open is made because of the difference in required time for both of these actions. If valves are already modulated open corresponding to the error signal at the time a trip open signal is generated, no additional trip action takes place.

Since the steam dump system requires a finite time to act, an increase in T_{avg} is to be expected. Lead/lag compensation for T_{avg} increases

the effect of T_{avg} on the error, thereby compensating for the lags in thermal response and valve positioning.

The rod control system, also acting on the $T_{avg} - T_{ref}$ error signal, reduces reactor power by control rod insertion. As T_{avg} approaches its new setpoint steam dump is reduced. The valves are fully seated when the deviation is small enough to be handled by the rod control system alone.

In order to prevent actuation of steam dump on small load perturbations, a block is provided which prevents valve response to either the trip or modulate signal unless a turbine load reduction has occurred. All elements of this channel, including the turbine impulse chamber pressure tap, are independent of the steam dump control system described above. A rate/lag unit in this channel generates an output proportional to the rate of decrease in turbine load. This output, when indicating a load rejection greater than 10% step or 5%/minute ramp, removes the block. Once unblocked, this block is manually reset. Manual control of steam dump also removes this block.

Turbine Trip Control

Because of the large heat capacity of the Reactor Coolant System and the high T_{avg} at full load, the steam generator safety valves would open following a turbine trip if there were no other means of removing the stored heat. Condenser steam dump and subcooled feedwater flow

are used to bring the plant to thermal no-load equilibrium without steam release to atmosphere.

Following a turbine trip, monitored by loss of turbine autostop oil pressure, the load rejection steam dump controller is defeated and the plant trip controller becomes active. In the T_{avg} control mode, the error signal is $T_{avg} - T_{no-load}$, and steam dump is proportional to this signal. The same error signal is used for on-off control of the feedwater control valve, as described in 3.4, Steam Generator Level Control. As T_{avg} is reduced to its no-load setpoint, steam dump is reduced and feedwater is shut off. As in the case of a load rejection, if the error signal exceeds the HI setpoint, a trip signal is generated which trips open four of the eight valves to their fully-open position. At the occurrence of a HI-HI trip signal, all eight valves trip open. Generally, the valves are not closed completely because of decay heat. No-load conditions are established within two minutes.

Pressure Control

For long term removal of residual heat at hot shutdown, or during plant startup or cooldown, the plant operator can manually switch to steam header pressure control. In this control mode, condenser steam dump acts to maintain a preset pressure in the steam header. A manual station is provided so that the operator can adjust the setpoint pressure or manually position the valves.

3.2.2 ATMOSPHERIC STEAM RELIEF SYSTEM

Atmospheric steam relief valves are mounted on the steam mains upstream of the steam line isolation valves. At the set pressure for these valves (about 1050 psig), their total capacity is 10% of maximum calculated turbine steam flow. These valves are modulating with a linear characteristic and have provision for remote adjustment of the set pressure. Stroke time is less than 20 seconds.

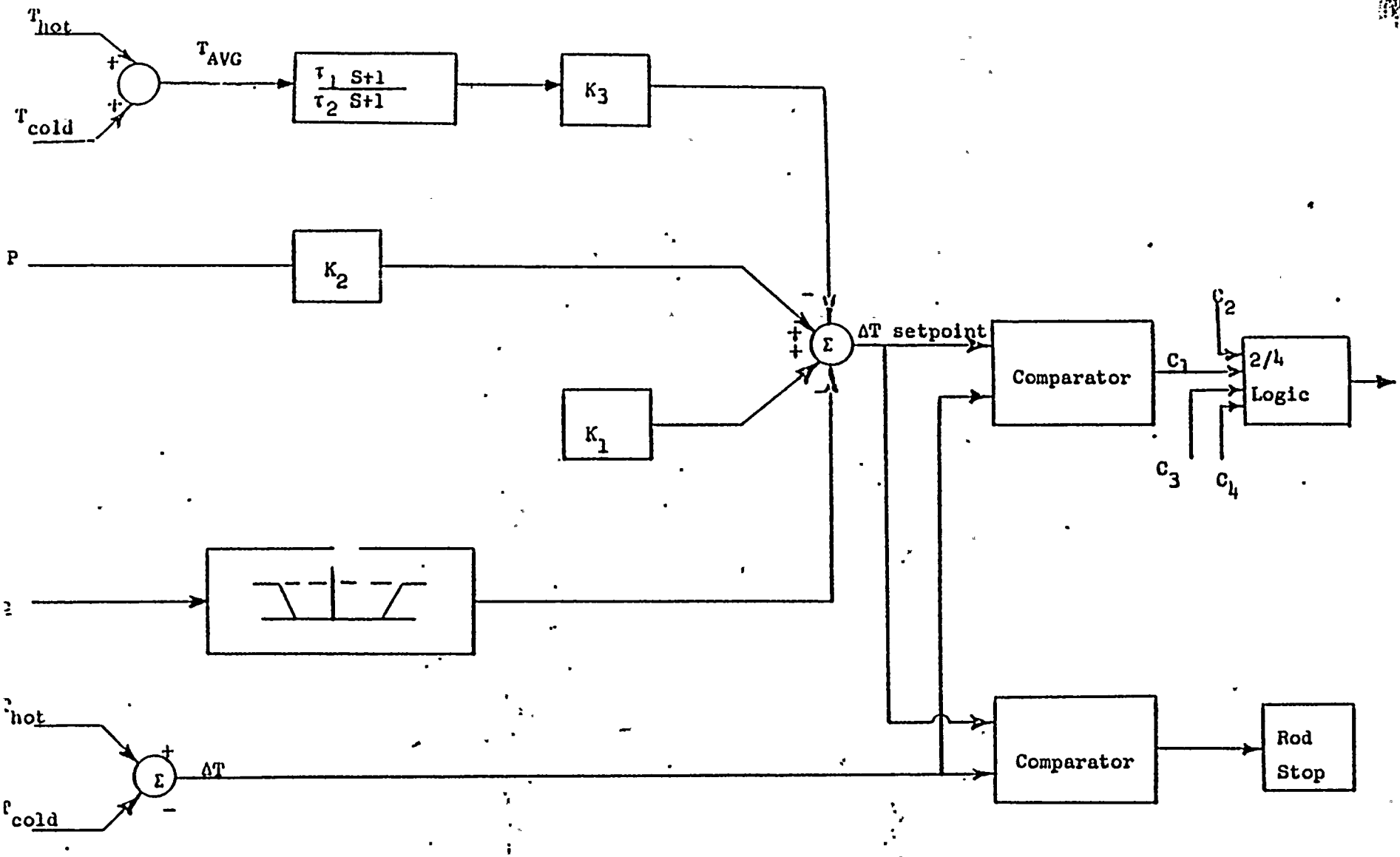
Atmospheric steam relief is provided to reduce service on the steam generator safety valves and to permit a plant cooldown when condenser steam dump is not available. These functions are explained below.

a) If a plant trip is caused by loss of condenser vacuum, condenser dump is blocked. The steam generator safety valves are available to remove stored energy from the Reactor Coolant System. Atmospheric steam relief reduces the steam pressure below the safety valve set pressure within two minutes after the trip. This prevents continuous chattering of the safety valves as residual heat is removed from the reactor.

b) Plant cooldown is accomplished by steam dump. If condenser dump is not available, the atmospheric relief is adequate to cool down to the temperature and pressure at which the residual heat removal system can be used.

c) In the event of a plant trip caused by an overpower/overtemperature condition or by a failure in the feedwater system, the atmospheric steam dump provides additional relief capacity, reducing the probability of safety valve actuation.

Separate controllers are provided for the atmospheric dump valves on the two steam generators, permitting independent pressure regulation if the steam generators are isolated.



OVERTEMPERATURE ΔT CHANNEL
(ONE CHANNEL OF FOUR SHOWN)
FIGURE 3.1-1

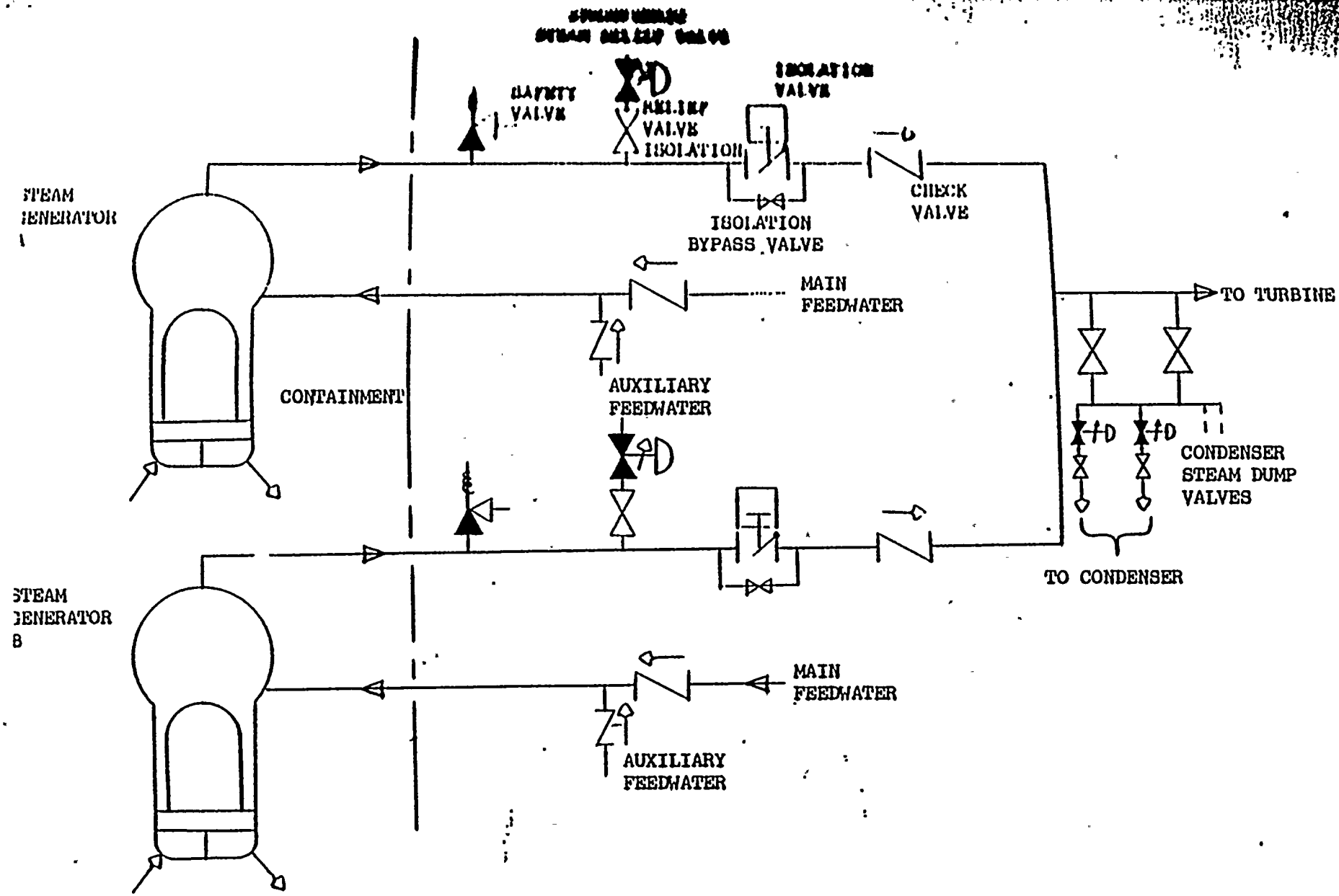


Figure 3.2-1

STEAM CYCLE VALVE ARRANGEMENT

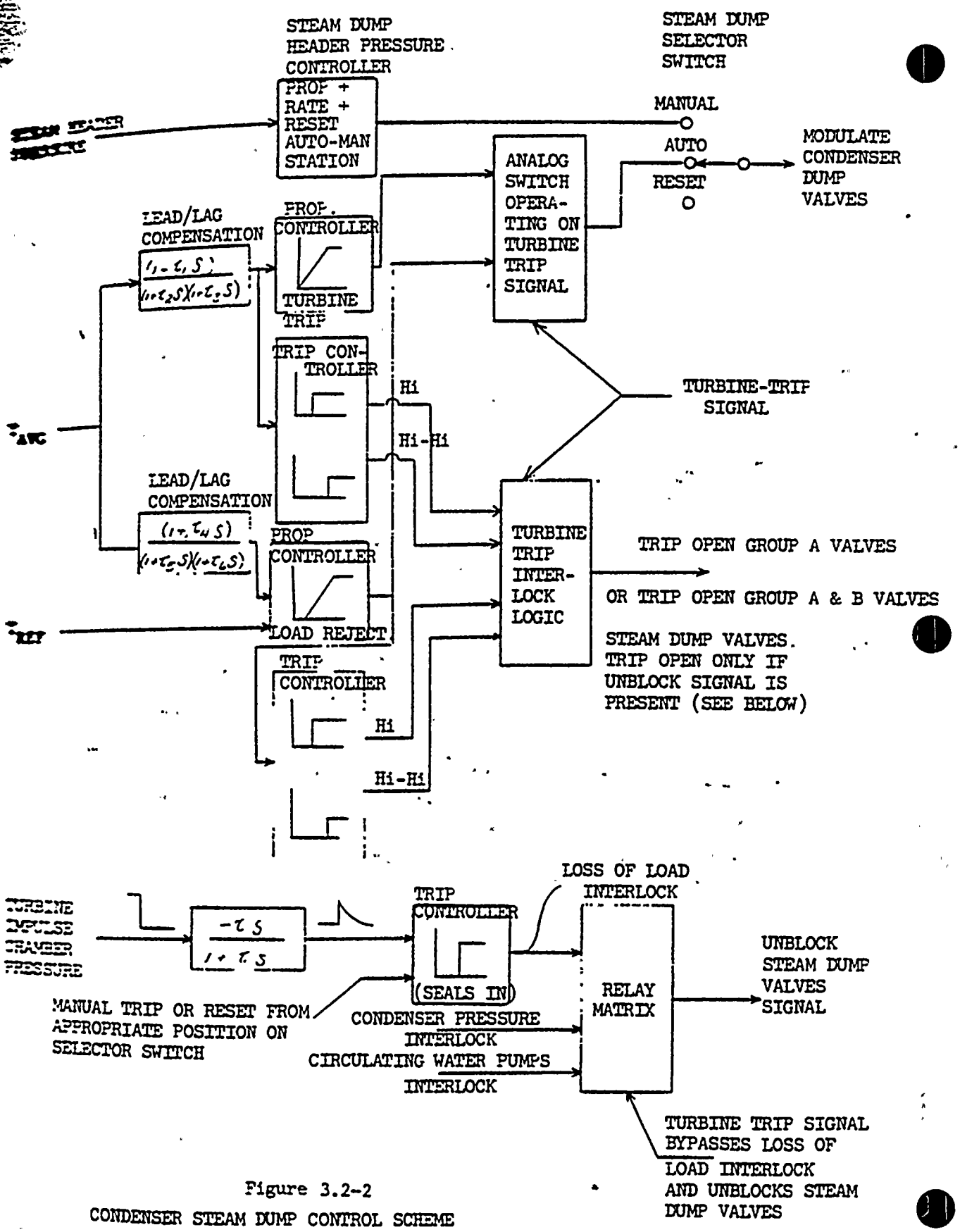


Figure 3.2-2

CONDENSER STEAM DUMP CONTROL SCHEME

3.3 REACTOR CONTROL

The basic Reactor Control System consists of three channels, which are temperature (T_{avg}), power mismatch ($Q_T - Q_n$) and reactor coolant pressure (P). The output of these three channels is used to drive the control rods via the rod program. A schematic representation of the control system is given in Figure 3.3-1.

The functions of each of these channels are as follows:

a) To maintain the programmed T_{avg} as accurately as possible

b) To be responsive to load perturbations without causing undue movement and reactor trips

c) To take corrective action in the case of large load changes if the pressure exceeds the limits of the normal pressure control.

The Temperature Channel

The temperature channel functions to maintain the programmed temperature (T_{avg}) as accurately as possible. The main requirements of this channel are that it should be accurate, stable and repeatable. This is the dominant control channel in steady-state conditions.

The Power Mismatch Channel

The power mismatch channels provide control stability and fast response to load perturbations. The output is proportional to the mismatch between turbine power and nuclear power. A high-pass filter in this channel ensures that steady-state calibration errors in the input power signals has no effect on steady-state control.

Another requirement of this channel is that its steady-state output should be zero even though a fixed offset in power signals may exist.

The Pressure Channel

This channel is provided to prevent large pressure changes following a large change in power. It retards the rate at which the controller changes T_{avg} to its new programmed set point. (If T_{avg} were to be changed too rapidly, pressurizer pressure control might not be able to maintain pressure within the normal operating range.)

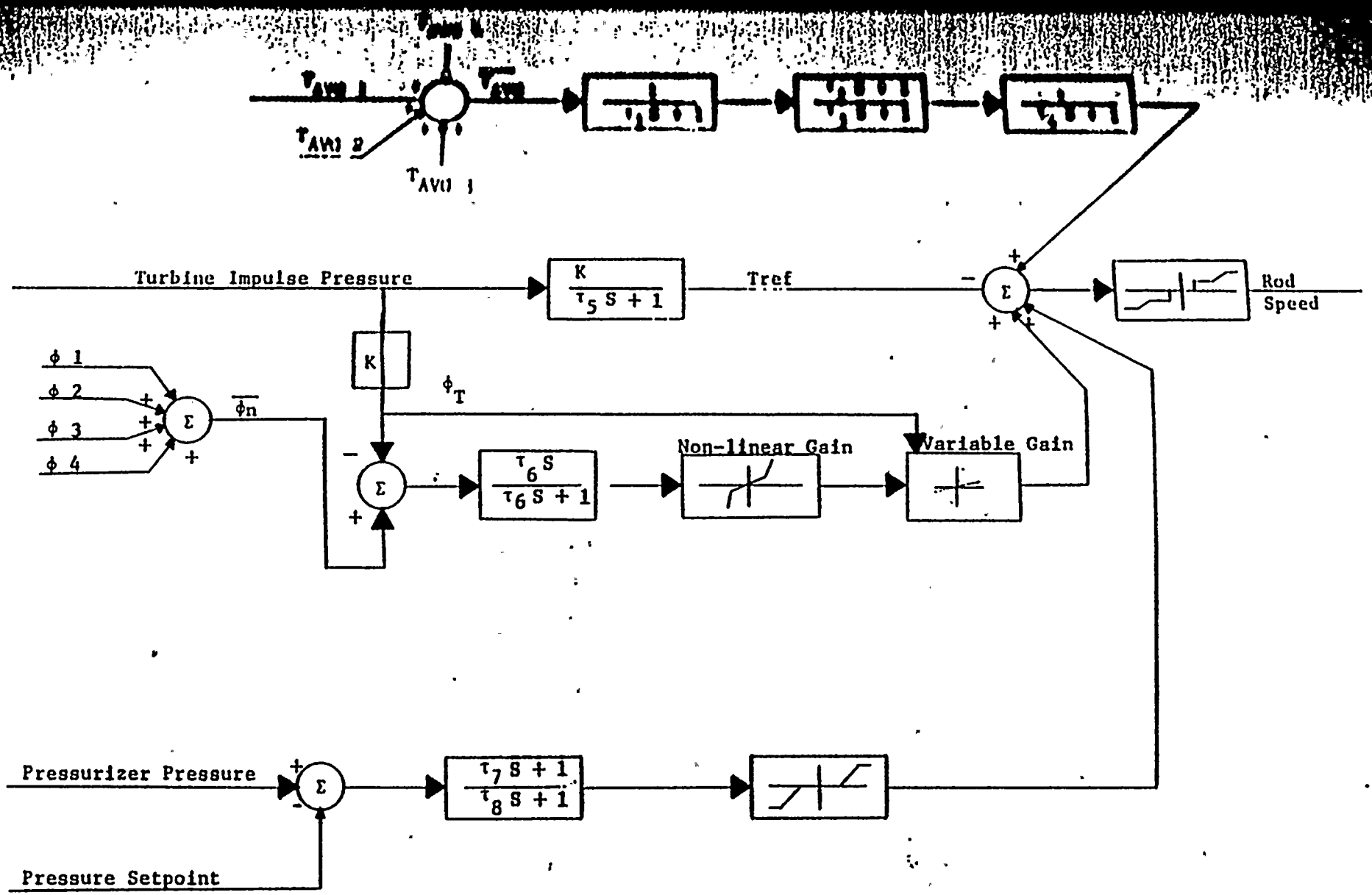
The pressure control channel has an adjustable deadband, so that only large pressure changes have an effect on rod motion.

This channel is not required for initial plant operation.

The Rod Speed Program

The rod speed program is made up of four parts: an adjustable deadband, a minimum speed, a proportional speed, and a maximum speed. The maximum speed is dictated by the mechanism design. All the other settings are adjustable. Expected set points are $\pm$ 1.5°F for the deadband and $\pm$ 5°F for maximum rod speed demand.

The outputs from the three channels mentioned above feed into the summing amplifier associated with the rod program.



REACTOR CONTROL SYSTEM
Figure 3.3-1

3.4 STEAM GENERATOR LEVEL CONTROL

In normal operation, the position of the main feedwater control valve is controlled by the three-element controller (feedwater flow, steam flow, water level). At low loads a bypass control valve is used.

The setpoint of the level controller is a function of load, programmed to rise with load between 0% and 20% load. A deviation alarm provides continuous monitoring of the level channel used for control versus the programmed level.

All narrow-range level channels are indicated. The wide-range level channel is recorded.

The steam flow and feedwater flow signals are supplied by either of two transmitters as selected by a control board mounted selector switch. The steam and feedwater flow signals used for control are recorded on a two-pen recorder.

Following a turbine trip, automatic control of the feedwater valve is switched from the three-mode level controller to on-off T_{avg} control. All feedwater control valves under automatic control are fully opened to admit maximum feedwater, then fully closed as no-load T_{avg} is approached to avoid excessive cooldown of the Reactor Coolant System.

Manual control of feedwater control valve position is available at the control board. This mode of control overrides automatic control on either level or T_{avg}.

In order to prevent excessive moisture carryover caused by high steam generator water level, a signal of high water level overrides all other control and closes the feedwater control valve. The signal is obtained from coincidence of two-of-three level channels above a preset value. This override is automatically removed from the main control valves as the water level drops below the set value. Manual reset is required for the bypass control valve.

The signals affecting feedwater valve control, in increasing the order of priority, are listed below:

a) Three-element level control or on-off T_{avg} control (dependent on whether or not turbine is tripped)

b) Manual control

c) High level override (closes feedwater valves)

d) Safety Injection System actuation (closes feedwater valves).

A wide-range level channel, calibrated for no-load conditions, is provided to allow manual control at hot shutdown and is also useful at cold shutdown. This channel includes a recorder.

3.5 STEAM BREAK PROTECTION SYSTEM

3.5.1 SAFETY INJECTION SYSTEM ACTUATION

The means of actuating the Safety Injection System have been noted in Section 3.1.2. Those particularly concerned with steam line break protection are low steam line pressure and high containment pressure.

The low steam line pressure signal is generated by the coincidence of two-of-three channels below approximately 500 psig for either steam line.

The high containment pressure signal is generated by the coincidence of two-of-three channels above approximately ten per cent of containment design pressure.

3.5.2 FEEDWATER LINE ISOLATION

Any safety injection signal isolates the main feedwater lines by closing all four main control valves, tripping the main feedwater pumps, and closing the pump discharge valves.

3.5.3 STEAM LINE ISOLATION

a) High steam flow in coincidence with any safety injection signal closes the isolation valve in that steam line.

   1. One-out-of-two steam flow signals above a HI-HI trip point (approximately 120% of full load steam flow)
   2. One-out-of-two steam flow signals above a HI trip point (approximately 20% of full load steam flow) in coincidence with two-out-of-four low T_{avg} signals (below approximately 540°F)

b) The coincidence of two-of-three high containment pressure signals

c) Manual actuation.

4. PROTECTION AND CONTROL SYSTEMS DESIGN PRINCIPLES

4.1 PROTECTION SYSTEM FUNCTIONAL DESIGN

The general philosophy for functional design Protection System is to derive protection directly from the process variables of interest whenever possible. In this manner, safety limit protection is assured independent of the initiating accident.

The overtemperature high delta-T trip protects the core against Departure from Nucleate Boiling (DNB) for all combinations of pressure, temperature, power, and axial power distribution. Thus, this single trip prevents DNB for rod withdrawal accidents, boron dilution, xenon oscillations, and excessive load variations. Protection against other limits, such as excessive power density and system overpressure, is also provided by close monitoring of the variable of direct interest.

In certain cases, however, these general protection functions are not rapid enough, or complete enough, to assure protection against a specific accident, such as loss of coolant flow. In these cases, specific trip functions are provided, such as reactor coolant pump bus undervoltage and reactor coolant low flow.

For certain more credible transients, such as turbine trip, a reactor trip is derived from the initiating event - even though safety limits would not be exceeded if a reactor trip were delayed until an overpressure or over-temperature trip occurred. In this manner, undesirable excursions are prevented, rather than terminated.

Finally, certain protective functions are provided primarily to ensure the continuing integrity of plant component and piping systems. Examples include reactor trip on high pressurizer water level to protect safety valve relief piping, and reactor trip on loss of feedwater to any steam generator. (The nuclear safety requirement is to prevent complete loss of heat sink; i.e., loss of feedwater to all steam generators.)

For equipment design purposes, no distinction is made between the various categories of protection mentioned above. The same criteria and design practice are applied to all channels. Other alternatives are neither defensible nor practical, since all of these protective functions enhance nuclear safety and complement or supplement one another.

This approach requires an instrumentation system that measures, on a timely, accurate, and reliable basis, dominate nuclear plant process variables. Instrument ranges, sensitivity, and time response must be selected consistent with the range and variation of each variable monitored. Also, since many process variables are monitored, considerable overlap in protection functions is a natural consequence.

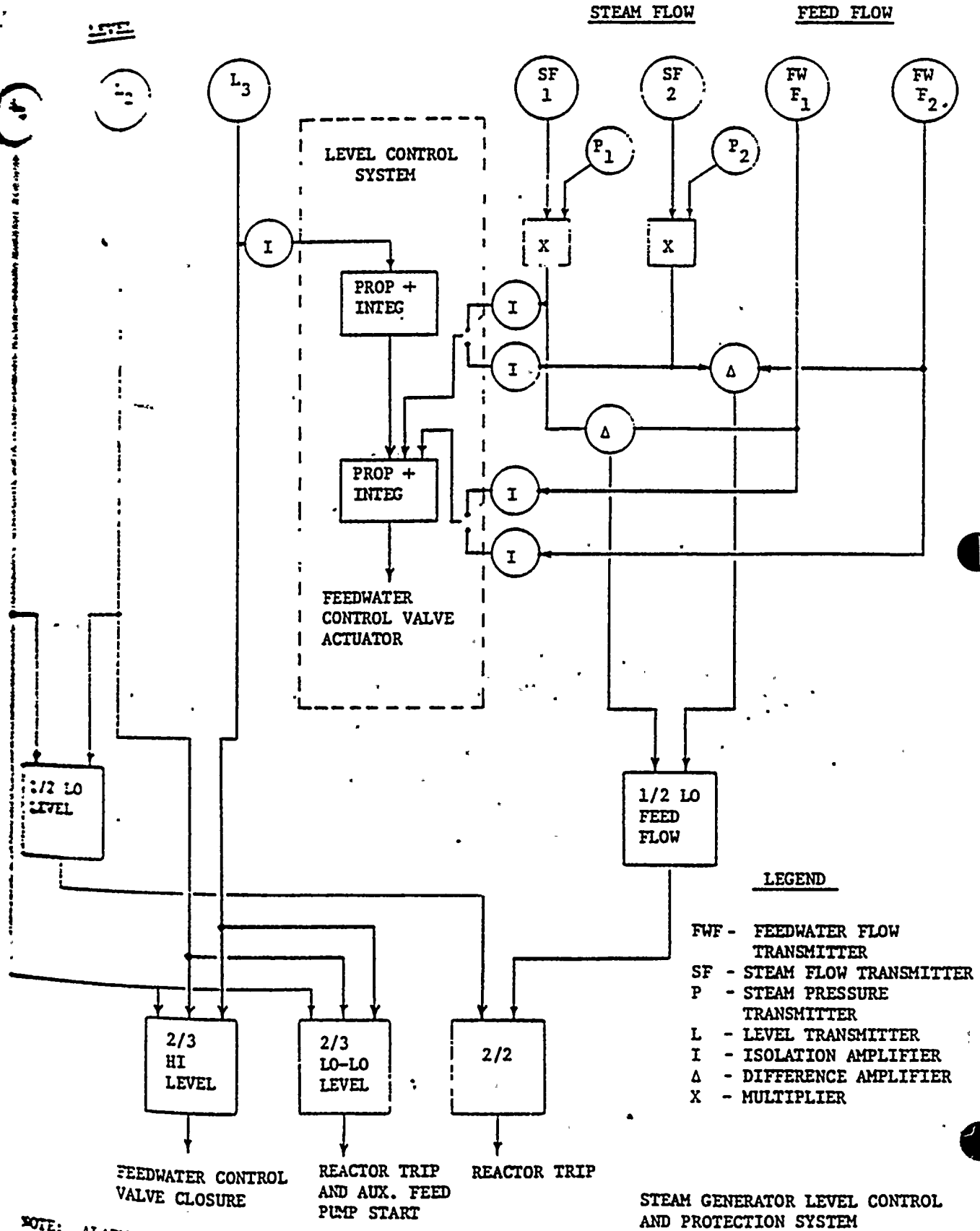
4.2 CONTROL SYSTEM FUNCTIONAL DESIGN

Power level and reactor coolant temperatures are controlled automatically in a Westinghouse PWR Plant. The reactor is controlled to follow any turbine load perturbation. This is ideal for load frequency control. The automatic Reactor Control System, therefore, forms an essential part of the plant operation. It is basically a regulating system which maintains proper steady-state operating conditions, thereby assuring adequate margins to trip settings for operational purposes and proper economic performance.

Other automatic control systems are pressurizer pressure and level control, feedwater control, and steam dump control. These systems are also essential to maintain normal operating conditions or to suppress excursions imposed by operational transients without recourse to protective action. As in the Protection System design, this requires an instrumentation system that measures, on an accurate, timely, and reliable basis, dominate nuclear plant process variables. These variables are, for the most part, the same as those required by the Protection System: loop temperatures, neutron flux, pressurizer pressure and level, steam generator level, steam flow and feedwater flow. In addition, the time response, instrument span, and sensitivity requirements for measurement channels serving each of the two systems are similar. As a result, primary sensor and transducing equipment that is acceptable for use with the Protection System should also be employed with the Control System.

Failure of the Control System to act when needed, or spurious actuation when not needed, generates a need for protection. The safest plant is

recognized to be one that requires the least protection. For this reason, as well as the economic desirability of avoiding plant outages which could have been prevented by proper control actions, every effort is made to ensure reliable control. Wherever practical, control interlocks and/or redundant control devices are provided to ensure that control action takes place when needed - but only when needed. Controller-induced excursions caused by a single sensor failure are largely eliminated in Westinghouse design practice.



NOTE: ALARMS AND INDICATORS NOT SHOWN.

STEAM GENERATOR LEVEL CONTROL AND PROTECTION SYSTEM

FIGURE 4.2-1

4.3 CONTROL AND PROTECTION INTERRELATION

In current Westinghouse PWR systems, the Protection and Control Systems are separate and distinct and are identified as such. The Control System, however, is dependent on signals derived from the Protection System through isolation devices. However, there is no feedback from the Control System to the Protection System.

The equipment design philosophy, illustrated on Figure 2-1, is that the Control System sensor is the output of the isolation amplifier. By this principle, no components are shared - they are either part of the Protection System and are located and designed as such, or they are part of the Control System. This is a very important feature of the Westinghouse design, and permits a dividing line, both functionally and physically, to be drawn between control and protection. It also ensures that inadvertent or deliberate changes to the Control System have no more effect on the Protection System than if the Control System contained independent sensors.

The design requirement for the analog isolation amplifiers is to isolate the Protection System from any electrical faults which might occur in the Control System. Extensive tests were performed to demonstrate this capability. In these tests, shorts, grounds, and a-c and d-c voltages were applied to the amplifier output. Even though some of these tests were destructive (i.e., destroyed the ability of the amplifier to produce a meaningful output signal), in no case was any perceptible disturbance fed back into the input circuit and hence to the Protection System.

The presence or absence of regulating control devices on the downstream side of the isolation amplifier has no effect on the isolation requirements. The same equipment and design requirement would exist even if these signals were brought out of the Protection System merely for remote readout and data-logging purposes. Since channel isolation cannot be reliably maintained on the control board or at the input terminals to a data-logger, an isolation device (amplifier or impedance network) in the protection channel represents the only feasible way to preserve protection channel independence.

Certain failures in the Protection System could conceivably negate a particular channel of a protective function, simultaneously causing spurious control action that might require protective action from that same function to prevent the excursion from exceeding design limits. Such possible failure is dealt with in accordance with the proposed standard, "Criteria for Nuclear Power Plant Protection Systems", IEE No. 279, Section 4.7, which requires that for such a fault, a second failure be assumed in the Protection System. In most cases in which control is derived from protection, Westinghouse design meets this criterion by providing a two-out-of-four Protection System logic. For example, as shown in Figure 4.3-1, a failure can be assumed in Protection Channel 1 which causes that channel to indicate high. This defeats the low pressure reactor trip for the channel, and also may cause the Pressure Control System (relief valves and spray) to rapidly reduce pressure. However, three of the pressure protection channels are left intact, and a reactor trip would automatically occur when any two of them reached the low pressure trip point.

In other cases, this additional redundancy is not necessary because such a failure cannot cause the safety limits to be exceeded. This fact can also be illustrated by Figure 4.3-1. A loss of signal (low indication) can be assumed for Protection Channel 1. This defeats the high pressure trip for that channel and may also energize the pressurizer heaters, causing a slow increase in pressure. If an independent failure is assumed in Channel 2, no reactor trip would occur when the pressure reached the high pressure trip setpoint since only one of the three high pressure trip channels is left intact. However, under this condition the safety valves on the pressurizer are more than adequate to ensure that the high pressure safety limit is not exceeded.

Section 4.4 discusses all such control and protection interactions for a specific plant design. In that section, it is noted that numerous operational defenses against these failures exist in addition to the primary or "protection grade" defense. Many of these additional barriers to an undesirable excursion are made possible by making redundant information available to the Control System.

The possibility of common-mode failure cannot be completely ruled out; it is conceivable that all identical channels behave identically, but incorrectly. In this case, the question of Control System dependence on the Protection System is irrelevant. It has been recognized that little, if any, additional degree of protection is achieved by having separate, but identical, instrument channels for control and protection. Indeed, Westinghouse considers that separation in this manner actually deprives the Protection System of

some of the day-by-day, hour-by-hour surveillance given to instrument channels needed for routine plant operation. A further, although often ignored disadvantage of proliferation of identical channels, is the attendant increase in visual displays and information processing problems of significant proportions. (Timely, accurate and complete information readout is required by the IEEE criteria previously referenced.)

A frequently expressed concern is the need for assurance that the Protection System will not be inadvertently modified during the 40-year life of the plant. This is occasionally cited as an argument against control dependence on Protection System information. Westinghouse completely agrees that every precaution must be taken to ensure adequate review of any future modification that could affect the Protection System.

Such assurance can only be achieved by complete attention to details in Protection System design, operation and maintenance. This must include identification of system components on drawings and on the equipment, documentation of the system design and design basis, and establishment of groups to review all proposed instrument changes that could affect plant safety or plant operations. It is fallacious to believe that independent control adds to this assurance. In fact, such independence could decrease the probability that a necessary correction to the Protection System will be made. Inadequacy of controller design requires correction to allow plant operation to proceed; inadequacy of protection is sometimes discovered only after an incident.

Control System modifications may be required to improve plant operation. For example, a filter may have to be added to achieve stability. As a control modification, this would logically be performed in the Control System; i.e., downstream of the isolation devices separating the Control and Protection Systems. Physical separation and identification of equipment (separate racks for Control and Protection Systems) and administrative precautions ensure that the logical route is, in fact, the one used.

Even advocates of complete independence between control and protection recognize the desirability and feasibility of using protection signals for non-protective functions. This introduces the possibility of these signals being diverted for other purposes unless a careful review and adherence to design bases is enforced.

The division between control and protection is not always clear. This reflects difficulty in defining the function achieved, rather than in equipment design implementation. Definitions that place all reactor trip and safeguards actuation instrumentation in the Protection System, and all automatic regulating instrumentation in the Control System, clearly leave many important items in between. Another definition advanced is that the Control System is "all instrumentation which is not protection," and the Protection System is "that instrumentation which must work when needed (to prevent unacceptable consequences)." This latter definition has considerable merit for general discussions and is useful in judging whether or not a particular item is a "protection" item or not. However, if taken as a rigid rule, it is difficult to apply to all design details, as is shown below.

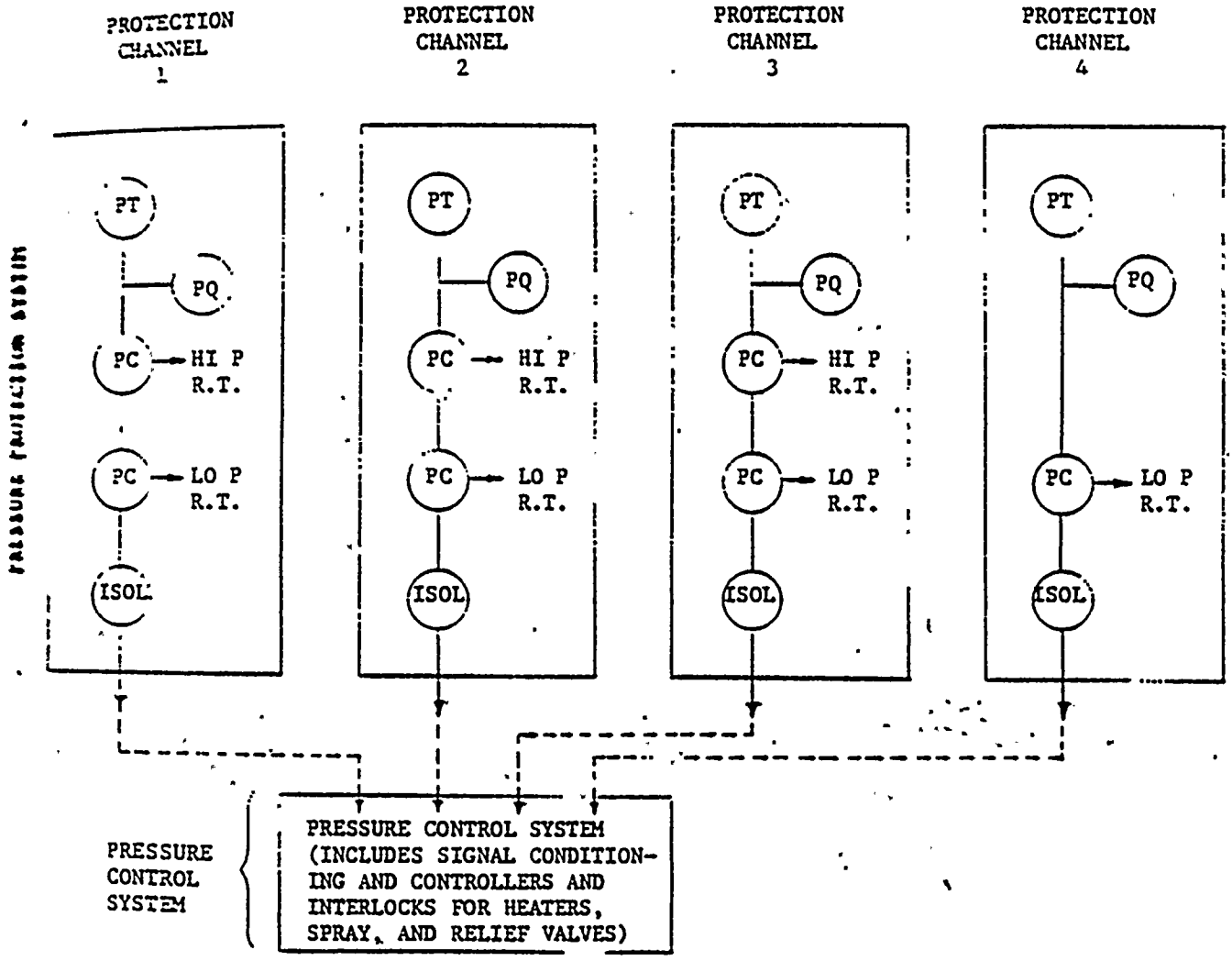
For example, alarms and/or control room indications derived from protection channel information are essential if the operator is to be properly and continuingly informed of the Protection System status and the status of plant safety. As previously noted, these alarms and indications are required by the referenced IEEE criteria as a vital part of the Protection System. In order to maintain protection channel isolation, Westinghouse equipment design practice associates remote indication with the output of the isolation device.

Other functions, such as control interlocks (e.g., rod stops) are often highly desirable, and may even be essential to plant safety if a number of malfunctions or maloperations should occur simultaneously (i.e., beyond the normal design groundrules).

Westinghouse has used the term "supervisory" for that category of functions that is neither clearly control or protection. (This is a functional designation only, and does not imply a third category for equipment design.) Supervisory functions can be further subdivided into two types: those that are informative only (indicators, recorders, alarms, and data-logging); and those which automatically act to arrest deteriorating conditions before protective action is needed. (This latter type has been termed "override", or "protective override".) Since the question is one of whether manual or automatic intervention is intended, the value of distinction is limited to failure mode analysis of automatic controllers.

Westinghouse recognizes that each "supervisory" function must be considered on its own merits to determine if it should form part of the Protection or the Control System.

A complete list of protection, control, and "supervisory" functions is included in the Appendix.



PT - PRESSURE TRANSMITTER
PQ - POWER SUPPLY
PC - CONTROLLER
ISOL - ISOLATION AMP
HI (LO) R.T. - HIGH (LOW) PRESSURE REACTOR TRIP

——— PROTECTION SYSTEM COMPONENTS
——— CONTROL SYSTEM COMPONENTS

NOTE: ALARMS, INDICATORS, AND RECORDERS ARE NOT SHOWN

PRESSURIZER PRESSURE PROTECTION AND CONTROL SYSTEMS DESIGN

FIGURE 4.3-1

4.4 SPECIFIC CONTROL AND PROTECTION INTERACTIONS

The design basis for the Control and Protection System permits the use of a detector for both protection and control functions. Where this is done, all equipment common to both the protection and control functions are classified as part of the Protection System. Isolation amplifiers prevent a Control System failure from affecting the Protection System. In addition, where failure of a Protection System component can cause a process excursion which requires protective action, the Protection System can withstand another, independent failure without loss of function. Generally, this is accomplished with two-out-of-four trip logic. Also, wherever practical, provisions are included in the Control or Protection System to prevent a plant outage because of single failure of a sensor.

The following discussion of specific control and protection interactions is based on the design for the Robert Emmett Ginna Nuclear Station of the Rochester Gas and Electric Co. (RGE). It is representative of current Westinghouse design practice.

4.4.1 NUCLEAR FLUX

Four power-range nuclear flux channels are provided for overpower protection. Isolated outputs from all four channels are averaged for automatic control rod regulation of power. If any channel fails in such a way as to produce a low output, that channel is incapable of proper overpower protection. In principle, the same failure could cause rod withdrawal and overpower. Two-out-of-four overpower trip logic insures an overpower trip if needed, even with an independent failure in another channel.

In addition, the Control System responds only to rapid changes in indicated nuclear flux; slow changes or drifts are overridden by the temperature control signal. Also, a rapid decrease of any nuclear flux signal blocks automatic rod withdrawal as part of the rod drop protection circuitry. Finally, an overpower signal from any nuclear channel blocks automatic rod withdrawal. The setpoint for this rod stop is below the reactor trip setpoint.

4.4.2 COOLANT TEMPERATURE

Four temperature channels, each containing a T_{avg} and a ΔT signal, are used for overtemperature-overpower protection. Isolated outputs from all four T_{avg} signals are also averaged for automatic control rod regulation of power and temperature. In principal, a spuriously low T_{avg} signal from one sensor would partially defeat this protection function and also cause rod withdrawal and overtemperature. Two-out-of-four trip logic is used to insure that an overtemperature trip occurs, if needed, even with an independent failure in another channel.

In addition, channel deviation alarms in the Control System block automatic rod motion (insertion or withdrawal) if any T_{avg} signal deviates significantly from the others. Automatic rod withdrawal blocks also occur if any one-of-four nuclear channels indicates an overpower condition or if any one-of-four temperature channels indicates an overtemperature or overpower condition. Finally, as shown in Section 14.1.2, of the RG&E Final Safety Analysis Report, the combination of trips on nuclear overpower, high pressurizer water level, and high pressurizer pressure also serve to limit an excursion for any rate of reactivity insertion.

4.4.3 PRESSURIZER PRESSURE

Four pressure channels are used for high and low pressure protection and for overpower-overtemperature protection. Isolated output signals from these channels also are used for pressure control and compensation signals for rod control. These are discussed separately below.

Control of Rod Motion

One of the pressure channels is used for rod control with a low pressure signal acting to withdraw rods. The discussion for coolant temperature is applicable; i.e., two-out-of-four logic for overpower-overtemperature protection as the primary protection, with backup from multiple rod stops and "backup" trip circuits. In addition, the pressure compensation signal is limited in the Control System such that failure of the pressure signal cannot cause more than about a 10°F change in T_{avg}. This change can be accommodated at full power without a DNBR less than 1.30. Finally, the pressurizer safety valves are adequately sized to prevent system overpressure.

Pressure Control

Low Pressure

A spurious high pressure signal from one channel can cause low pressure by spurious actuation of spray and/or a relief valve. Additional redundancy is provided in the Protection System to insure underpressure protection; i.e., two-out-of-four low pressure reactor trip logic and one-out-of-three logic for safety injection. (Safety injection is actuated on one-out-of-three coincident low pressure and low level signals.)

In addition, interlocks are provided in the Pressure Control System such that a relief valve closes if either of two independent pressure channels indicates low pressure. Spray reduces pressure at a lower rate, and some time is available for operator action (about three minutes at maximum spray rate before a low pressure trip is required.)

High Pressure

The pressurizer heaters are incapable of overpressurizing the Reactor Coolant System. Maximum steam generation rate with heaters is about 7500 lbs/hr., compared with a total capacity of 576,000 lbs/hr., for the two safety valves and a total capacity of 179,000 lbs/hr., for the two power-operated relief valves. Therefore, overpressure protection is not required for a pressure control failure. Two-out-of-three high pressure trip logic is used.

In addition, either of the two relief valves can easily maintain pressure below the high pressure trip point. The two relief valves are controlled by independent pressure channels, one of which is independent of the pressure channel used for heater control. Finally, the rate of pressure rise achievable with heaters is slow, and ample time and pressure alarms are available for operator action.

4.4.4 PRESSURIZER LEVEL

Three pressurizer level channels are used for high level reactor trip (2/3) and low level safety injection (1/3 logic level coincident with pressure). Isolated output signals from these channels are used for volume control, increasing or decreasing water level. A level control

failure could fill or empty the pressurizer at a slow rate (on the order of half an hour or more).

High Level

A reactor trip on pressurizer high level is provided to prevent rapid thermal expansions of reactor coolant fluid from filling the pressurizer; the rapid change from high rates of steam relief to water relief can be damaging to the safety valves and the relief piping and pressure relief tank. However, a level control failure cannot actuate the safety valves because the high pressure reactor trip is set below the safety valve set pressure. With the slow rate of charging available, overshoot in pressure before the trip is effective is much less than the difference between reactor trip and safety valve set pressures. Therefore, a control failure does not require Protection System action.

In addition, ample time and alarms are available for operator action.

Low Level

For control failures which tend to empty the pressurizer, one-out-of-three logic for safety injection actuation on low level insures that the Protection System can withstand an independent failure in another channel.

In additon, a signal of low level from either of two independent level control channels isolates letdown, thus preventing the loss of coolant. Also, ample time and alarms exist for operator action.

4.4.5 STEAM GENERATOR WATER LEVEL FEEDWATER FLOW

Before describing control and protection interaction for these channels, it is beneficial to review the Protection System basis for this instrumentation. The system is shown schematically in Figure 4.4-1.

The basic function of the reactor protection circuits associated with low steam generator water level and low feedwater flow is to preserve the steam generator heat sink for removal of long term residual heat. Should a complete loss of feedwater occur with no protective action, the steam generators would boil dry and cause an overtemperature-overpressure excursion in the reactor coolant. Reactor trips on temperature, pressure, and pressurizer water level trip the plant before there is any damage to the core or Reactor Coolant System. However, residual heat after trip causes thermal expansion and discharge of the reactor coolant to containment through the pressurizer relief valves. This would breach one of the barriers -- the Reactor Coolant System -- to release of fission products. Redundant emergency feedwater pumps are provided to prevent this. Reactor trips act before the steam generators are dry to reduce the required capacity and starting time requirements of these pumps and to minimize the thermal transient on the Reactor Coolant System and steam generators. Independent trip circuits are provided for the two steam generators for the following reasons:

a) Should severe mechanical damage occur to the feedwater line to one steam generator, it is difficult to insure the functional integrity of level and flow instrumentation for that unit. For instance, a

major pipe break between the feedwater flow element and the steam generator would cause high flow through the flow element. The rapid depressurization of the steam generator would drastically affect the relation between downcomer water level and steam generator water inventory. However, the independent circuits on the second steam generator are sufficient to actuate a reactor trip if needed.

b) It is desirable to minimize thermal transients on a steam generator for credible loss of feedwater accidents.

Controller malfunctions caused by a Protection System failure affect only one steam generator. Also, they do not impair the capability of the main feedwater system under either manual control or automatic T_{avg} control. Hence, these failures are far from being the worst case with respect to core decay heat removal with the steam generators.

Feedwater Flow

A spurious high signal from the feedwater flow channel being used for control would cause a reduction in feedwater flow and prevent that channel from tripping. A reactor trip on low-low water level, independent of indicated feedwater flow, insures a reactor trip, if needed.

In addition, the three-element feedwater controller incorporates reset on level, such that with expected gains, a rapid increase in the flow signal would cause only a 12-inch decrease in level before the controller re-opened the feedwater valve. A slow increase in the feedwater signal would have no effect at all.

Steam Flow

A spurious low steam flow signal would have the same effect as a high feedwater signal, discussed above.

Level

A spurious high water level signal from the protection channel used for control tends to close the feedwater valve. This level channel is independent of the level and flow channels used for reactor trip on low flow coincident with low level.

a) A rapid increase in the level signal completely stops feedwater flow and actuates a reactor trip on low feedwater flow coincident with low level.

b) A slow drift in the level signal may not actuate a low feedwater signal. Since the level decrease is slow, the operator has time to respond to low level alarms. Since only one steam generator is affected, automatic protection is not mandatory and reactor trip on two-out-of-three low-low level is acceptable.

4.4.6 STEAM LINE PRESSURE

The three pressure channels per steam line are used for steam break protection (two-out-of-three low pressure signals for any steam line actuates safety injection). One of these channels is used to control the power-operated relief valve on that steam line. These valves are typically rated at 10% of the safety valve capacity. A spurious high pressure signal from the channel used for control opens the relief valve and causes low pressure. This is a slow rate of steam release, evaluated as a credible

steam break in Section 14.2.5 of the RG&E Final Safety Analysis Report. In the analysis of steam breaks of this size, no credit is taken for the steam line pressure instrumentation. Safety injection is actuated by the pressurizer instrumentation. Therefore, a control failure does not create a need for this protection, and two-out-of-three logic is acceptable.

5. ACCIDENT EVALUATION

5.1 ROD WITHDRAWAL ACCIDENT

The Protection System evaluation of the rod withdrawal accident is based on the MCZ plant parameters, protection system, and expected reactivity coefficients. The design basis for the Reactor Protection System to protect the core for rod withdrawal accidents is to trip the reactor before a 1.30 DNBR is reached in the hot channel. While diversity in types of instrumentation is not a part of the design basis, the system as provided does provide alarms, rod stops and control functions to prevent the withdrawal from proceeding to the trip point. Because of inherent effect of overpower on all the process variables, additional trip functions would act to terminate the excursion, but not necessarily before 1.30. Extending the course of the accident, a DNBR of 1.0 in the "hot assembly" is arbitrarily selected as a limit for a second level of protection. (The "hot assembly" is essentially the hot channel without allowance for engineering hot channel factors.) No credit is taken for power flattening or local void reactivity effects at overpower conditions. The most pessimistic instrument error and set points are assumed for all reactor trips.

Sustained overpower is of serious concern because of the potential damage to the core and the Reactor Coolant System. System overpressure is prevented by either the high pressure reactor trip or by the pressurizer safety valves in conjunction with any reactor trip on high power, temperature, or water level. The diversity for core damage is not so obvious, and this evaluation is focused on this concern.

The protection against the rod withdrawal leading to undesirable consequences is in considerable depth, and there are indeed multiple levels of protection as listed below. Each of these levels could be independently considered adequate, diverse protection against an accident.

a) Because the reactivity available by rod withdrawal is limited, only in very rare cases could complete rod withdrawal cause core damage. A single trip function with redundant channels protects against this condition. No diversity or separation is required.

b) Multiple, diverse rod stops are provided such that no failure can cause a sustained automatic rod withdrawal. Therefore, a reactor trip could be considered as backup protection.

c) For "fast" excursions, two reactor trip functions prevent all but limited core damage. For "slow" excursions, manual action is an adequate backup to the automatic protection system.

d) For all rod withdrawal accidents, at least two reactor trip functions exist, either of which would again prevent all but limited core damage.

Fault tree diagrams are shown on Figure 5.1-1 and 5.1-2.

5.1.1 PROBABLE CONSEQUENCES OF ACCIDENT

The adequacy, or depth, of protection required for an accident should be measured against the probability of the accident and the probable consequences of the unprotected accident. The probable consequences are discussed here.

The rod reactivity available is intentionally limited during operation for several reasons (equalize burnup, maintain shutdown margin, improve

power distribution, and reduce ejected rod worths). The design allowance for rod insertion at full power is 0.1% for "bite" plus 0.4% for the maneuvering band; i.e., rod insertion may be anywhere from 0.1% to 0.5%. With calculated values for moderator and power coefficients at beginning of core life*, 0.3% reactivity insertion is required to reach a hot assembly DNBR of 1.0. Also, after 20% core burnup, 0.5% insertion does not cause a hot assembly DNBR less than 1.0. Therefore, a random, complete rod withdrawal from design full power conditions with no protection has about 5% probability of causing DNBR less than 1.0. This is illustrated by Figure 5.1.3. Although the figure and the above discussion are based on full power, they are equally applicable to accidents starting from less than full power since the additional inserted rod worth is needed to achieve full power. However, it may not be practical to guarantee these conditions because allowances for calculation or measurement uncertainties can significantly affect the results. Figures 5.1.4 and 5.1.5 shows a "worst case" complete rod withdrawal at 25% of core life from 102% power, nominal T_{avg} plus 4°F, and nominal pressure less 30 psi. Reactivity insertion is assumed to be 0.6%, or 0.5% ± 1.2. (This 20% uncertainty could have been applied to the reactivity coefficients instead of the rod worth.) Minimum hot assembly DNBR is 0.91, or slightly less than the arbitrary limit of 1.0. The same transient at 60% of core life is shown for comparison. Minimum hot assembly DNBR is 1.46.

---

*Reactivity coefficients based on Figures 3.2.1-8 and 3.2.1-10 in Supplement 4 to the RGE FSAR, dated October 23, 1968.

A complete analysis, considering statistical variations in all uncertainties, would determine a more valid value or the probability of exceeding any given safety limit. If this value were sufficiently small, a comparatively "thin" protection system might be justified.

5.1.2 PROBABILITY OF ACCIDENT

The design intent of the Reactor Control System is to block automatic rod withdrawal for any failure which can cause sustained rod withdrawal. This is accomplished by rod stops on rapid nuclear flux decrease, T_{avg} channel deviation, spurious rod motion, and subsequent rod stops on high ΔT or high flux.

If rod stops were considered as independent protection, Protection System criteria would be applied. These rod stops would then be classified fully as part of the Protection System for a rod withdrawal accident.

5.1.3 MANUAL INTERVENTION

Manual action is reliable backup to automatic protection provided that sufficient time exists for operator response. The time required depends on the alarms available, the nature of the problem, and the required action.

Figure 5.1-6 illustrates steady-state core limits and several alarm points and trip points. Alarms are intentionally quite close to the design operating conditions. Other alarms such as high pressure would be reached during a transient. These alarms are tabulated on Table 5.1-1.

Although steam cycle heat removal may be the most limiting steady-state restriction on reactor power, time is required to reach corresponding

alarms and trip points. (For instance, it would take about two minutes at 110% reactor power with steam generator safety valves blowing before a steam generator low-low water level trip could be expected.) For this reason, this evaluation did not include these alarms and trips.

Figures 5.1-7 through 5.1-10 show the results of transient analysis for various reactivity insertion rates at beginning of core life from maximum full power (102%, nominal T_{avg} +4°F, nominal pressure less 30 psia), and from nominal conditions at 80% power. A constant reactivity insertion rate with unlimited available reactivity is assumed. Maximum settings and instrument errors are assumed for the reactor trips, and nominal set points for the alarms. (Note: the high ΔT rod stops are taken as 3°F below their reactor trips rather than their nominal set points.)

For a reactivity insertion rate of 0.5×10^{-4} δk./sec, (corresponding roughly to maximum rod speed at average rod worth), a hot assembly DNBR of 1.0 is reached in about two minutes. During this time, there are alarms on high T_{avg}, pressurizer pressure, and pressurizer level, as well as rod stops and alarms on high flux and high ΔT. Also, the steam safety valves would be actuated. With the multiplicity of alarms, it is easy to diagnose a major overpower-overtemperature excursion. It is reasonable to expect operator intervention (manual trip) during this time.

For faster reactivity insertion rates, reactor trip on high nuclear flux is a reliable protection system barrier. Therefore, since the overtemperature high ΔT trip protects for all excursions, one could classify it as the principal protection barrier with "backup" from high nuclear flux in conjunction with manual action.

5.1.4 DIVERSITY OF REACTOR TRIPS

The protection system design basis for the rod withdrawal accident for core protection required that one trip function with redundant channels prevent a minimum DNBR less than 1.30. This is accomplished with the overtemperature ΔT trip for slow reactivity excursions, and the high nuclear flux trip for fast excursions. As shown by Figures 5.1-7 through 5.1-10, these two trips meet the design basis.

The evaluation also shows that for all cases of sustained reactivity insertion for rates up to four times the maximum rate expected from rod withdrawal, any of the following prevent a hot assembly DNBR less than 1.0.

a) High nuclear flux reactor trip

b) High ΔT trip

   1. Overpower ΔT

   2. Overtemperature ΔT

c) High pressurizer level reactor trip plus high pressurizer pressure reactor trip. (Not valid for high reactivity insertion rates from near full power.)

This depth of protection cannot be expected for all accidents or for all plants.

TABLE 5.1-1

ALARMS FOR ROD WITHDRAWAL

The alarms which would be actuated for a spurious rod withdrawal accident near full power are listed below in the approximate order in which they would occur. Alarm points assumed for the evaluation are listed.

1. Initiating Fault* - Most failures which can cause a spurious control rod withdrawal are alarmed and, in general, automatic motion prohibited. These include:
   a) NIS flux rapid decrease (1/4) (5% in 5 seconds)
   b) T_{avg} channel deviation (1/4) ($\pm$5°F from average)
   c) Rod control fault - rod motion with no demand
2. Step Counter - audible clicks from step counter alerts operator to rod motion.
3. NIS PWR RANGE OVERPOWER ROD STOP* (1/4) (105%)
4. AVG T_{AVG} -T REF DEV (T_{avg} $\pm$5°F from program)
5. PRESSURIZER HI PRESSURE (2350 psia)
6. PRESSURIZER RELIEF LINE HI TEMP (when power-operated relief valves open)
7. REACTOR COOL HI T_{AVG} (1/4) (5° above nominal T_{avg} at full power)
8. PRESSURIZER LEVEL DEVIATION (5% above programmed level at full power)
9. AUTO TURBINE RUNBACK OVERPOWER ΔT* (1/4) (3°F less than high ΔT trip point)
10. AUTO TURBINE RUNBACK OVERTEMP ΔT* (1/4) (3°F less than high ΔT trip point)
11. Steam Generator Relief and Safety Valve Actuation - audible steam release to atmosphere
12. STEAM GENERATOR LEVEL SET POINT DEVIATION
13. PRESSURIZER SAFETY VALVE OUTLET HI TEMP (2500 psia)
14. ... CHANNEL ALERT - as reactor trip points are reached for each channel

NOTE: Capitalized word groupings represent engraving on annunciator panels.

REACTOR TRIPS FOR ROD WITHDRAWAL

The following trip points were assumed for the evaluation:

1. NIS POWER RANGE HIGH RANGE (2/4) (118%)
2. OVERPOWER ΔT (2/4) (118% of full power ΔT).
3. OVERTEMPERATURE ΔT (2/4) (variable)
4. PRESSURIZER HI PRESSURE (2/3) (2400 psia)
5. PRESSURIZER HI LEVEL (2/3) (95% of span)

---

* Alarm and Rod Stop

FAULT TREE FOR ROD WITHDRAWAL ACCIDENT

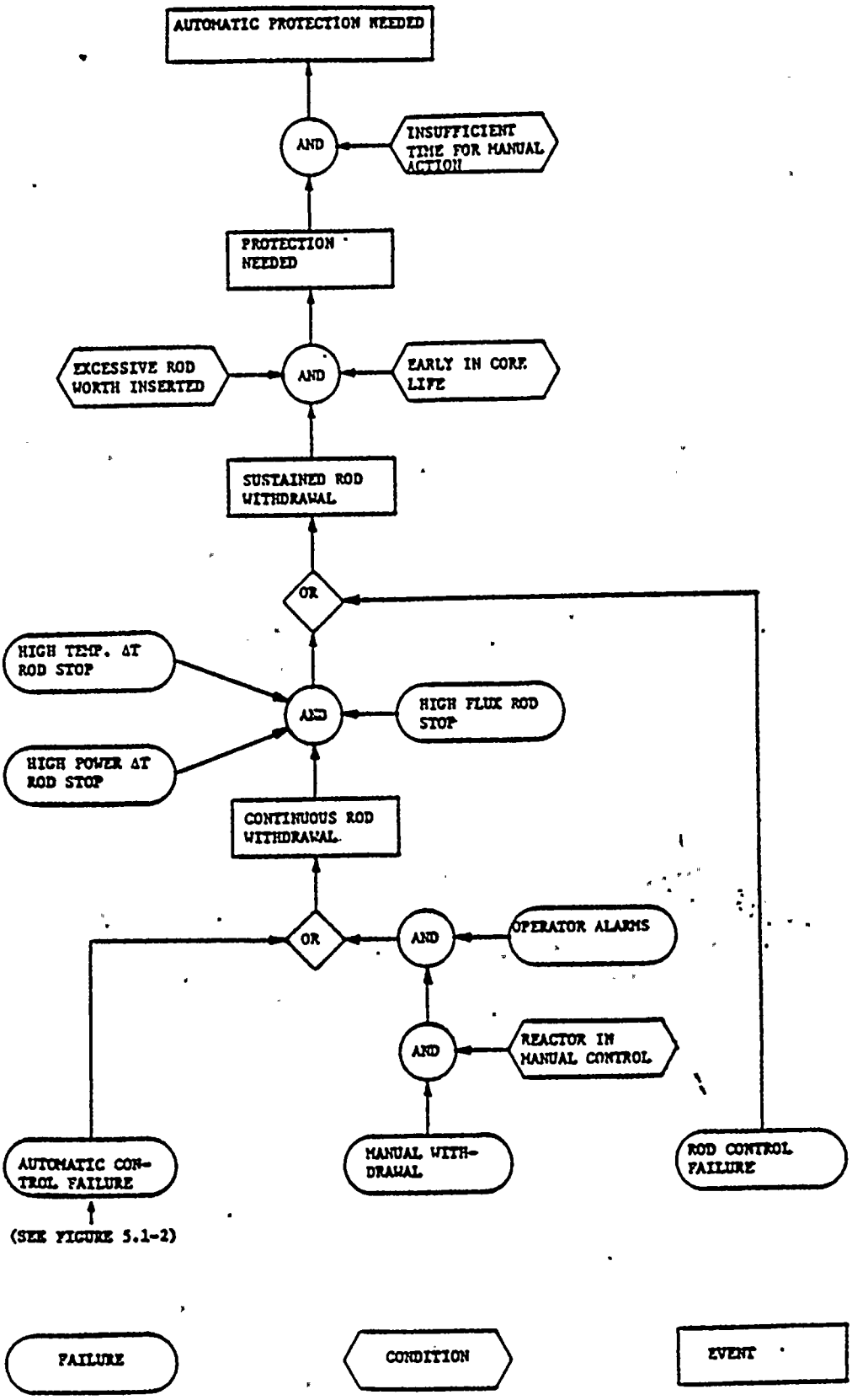


FIGURE 5.1-1

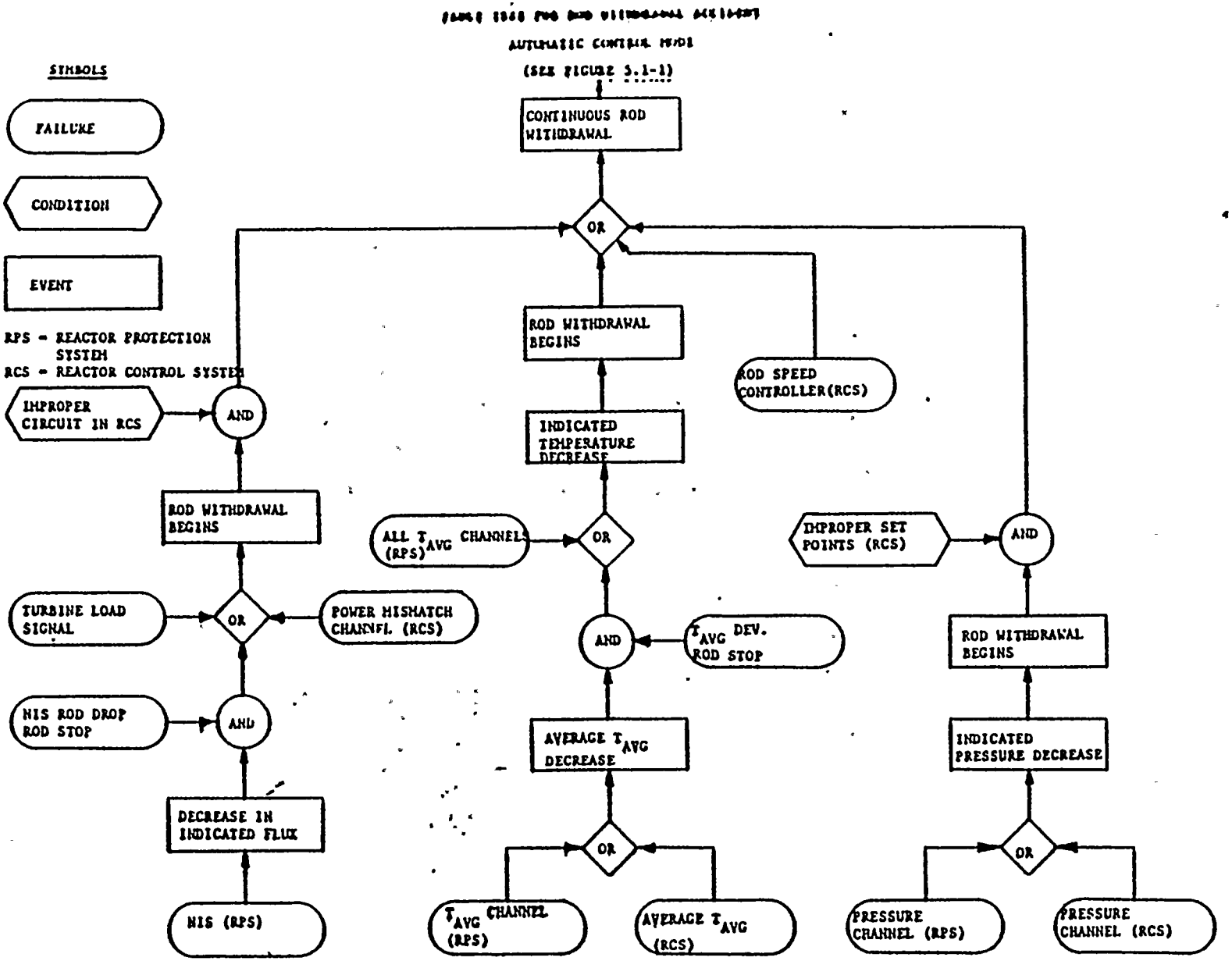

AUTOMATIC CONTROL MODE
(SEE FIGURE 5.1-1)
SYMBOLS
FAILURE
CONDITION
EVENT
RPS - REACTOR PROTECTION SYSTEM
RCS - REACTOR CONTROL SYSTEM
CONTINUOUS ROD WITHDRAWAL
OR
ROD WITHDRAWAL BEGINS
ROD SPEED CONTROLLER(RCS)
INDICATED TEMPERATURE DECREASE
ALL T_{AVG} CHANNELS (RPS)
OR
AND
T_{AVG} DEV. ROD STOP
AVERAGE T_{AVG} DECREASE
OR
T_{AVG} CHANNEL (RPS)
AVERAGE T_{AVG} (RCS)
IMPROPER CIRCUIT IN RCS
AND
ROD WITHDRAWAL BEGINS
TURBINE LOAD SIGNAL
OR
POWER MISMATCH CHANNEL (RCS)
NIS ROD DROP ROD STOP
AND
DECREASE IN INDICATED FLUX
NIS (RPS)
IMPROPER SET POINTS (RCS)
AND
ROD WITHDRAWAL BEGINS
INDICATED PRESSURE DECREASE
OR
PRESSURE CHANNEL (RPS)
PRESSURE CHANNEL (RCS)

FIGURE 5.1-2

INSERTED ROD WORTH AND REACTIVITY REQUIRED TO REACH DNBR = 1.0 IN HOT ASSEMBLY VERSUS CORE LIFE

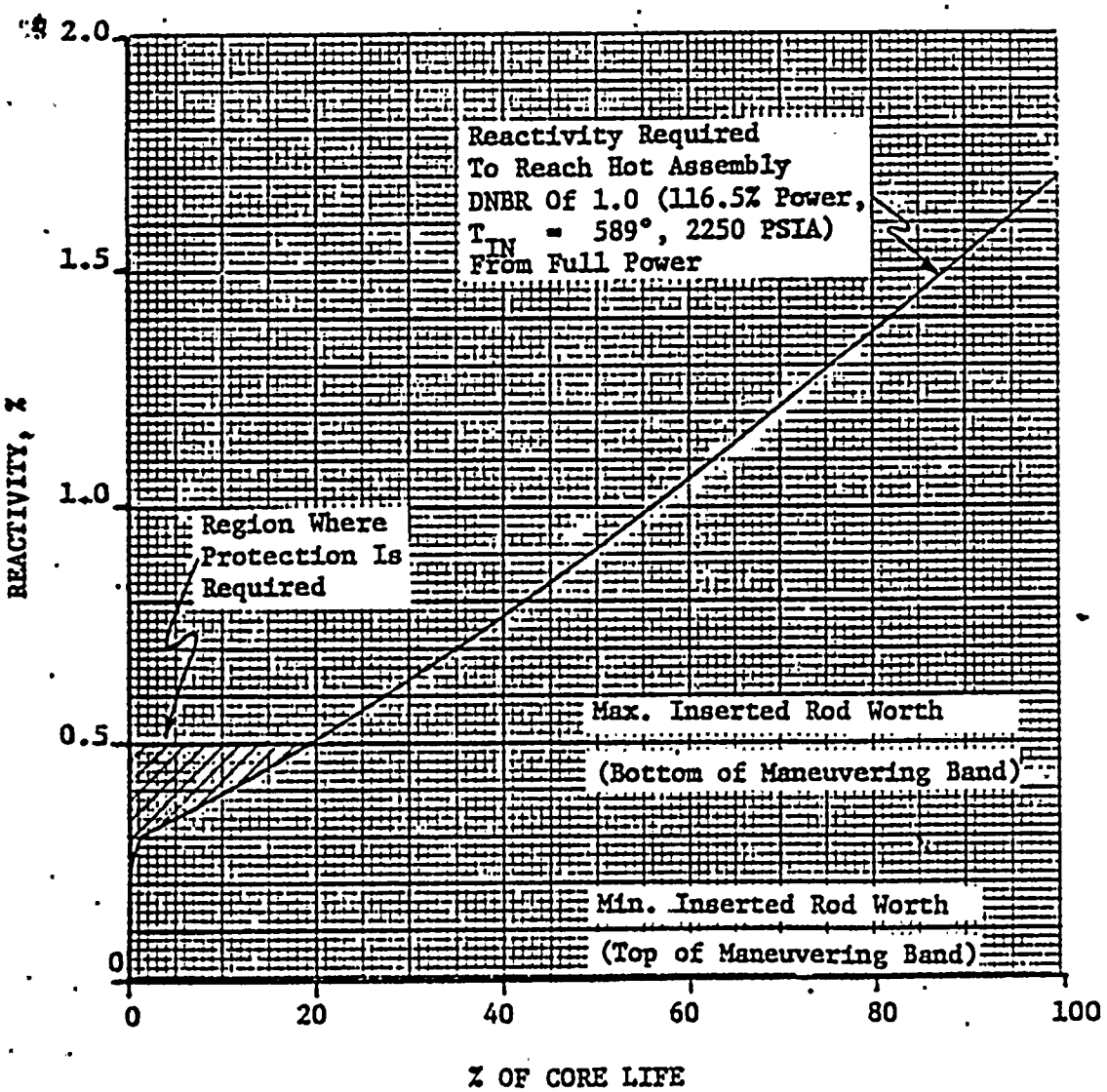
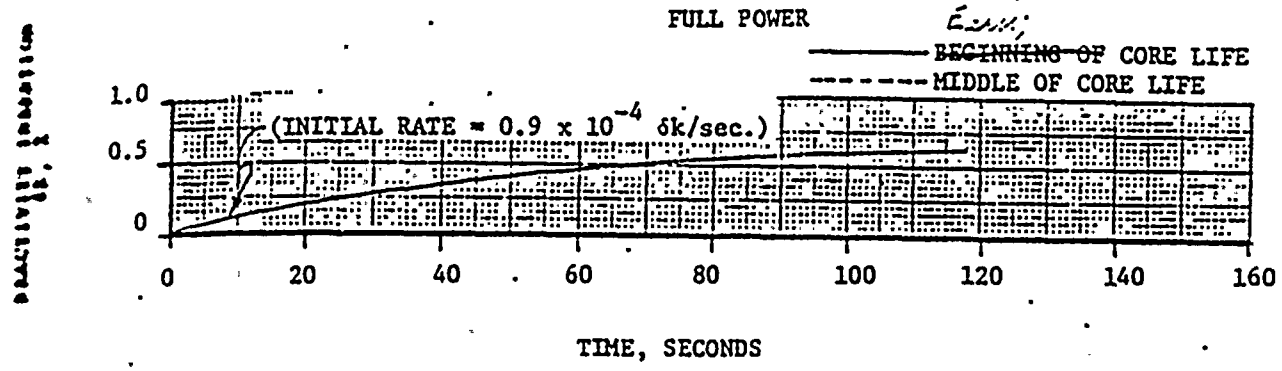
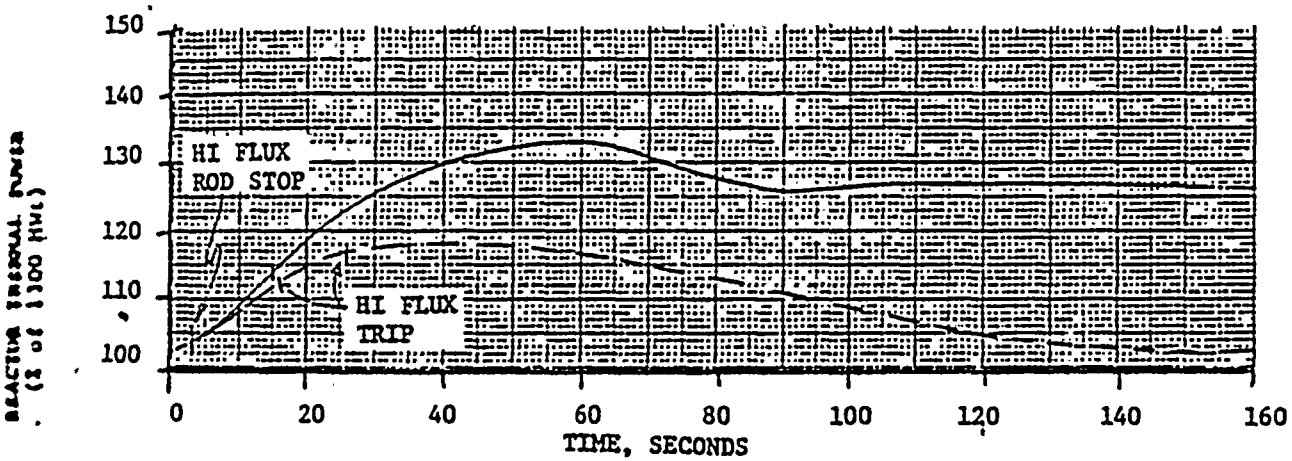
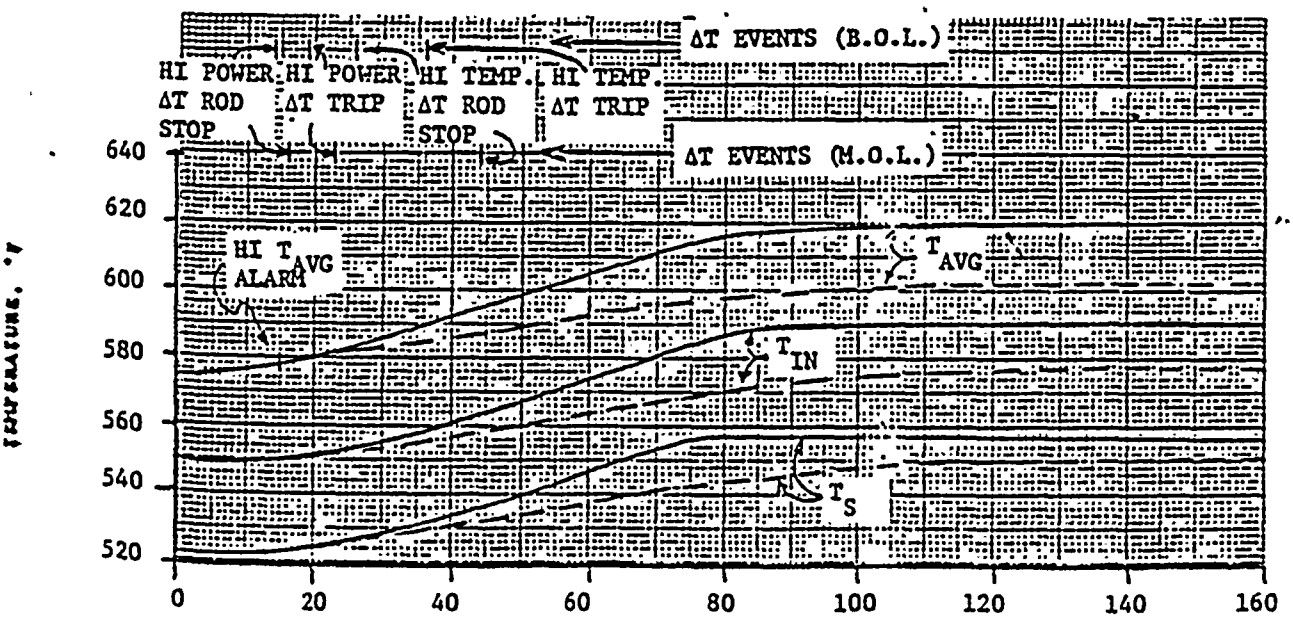


FIGURE 5.1-3

COMPLETE ROD WITHDRAWAL FROM MAXIMUM FULL POWER







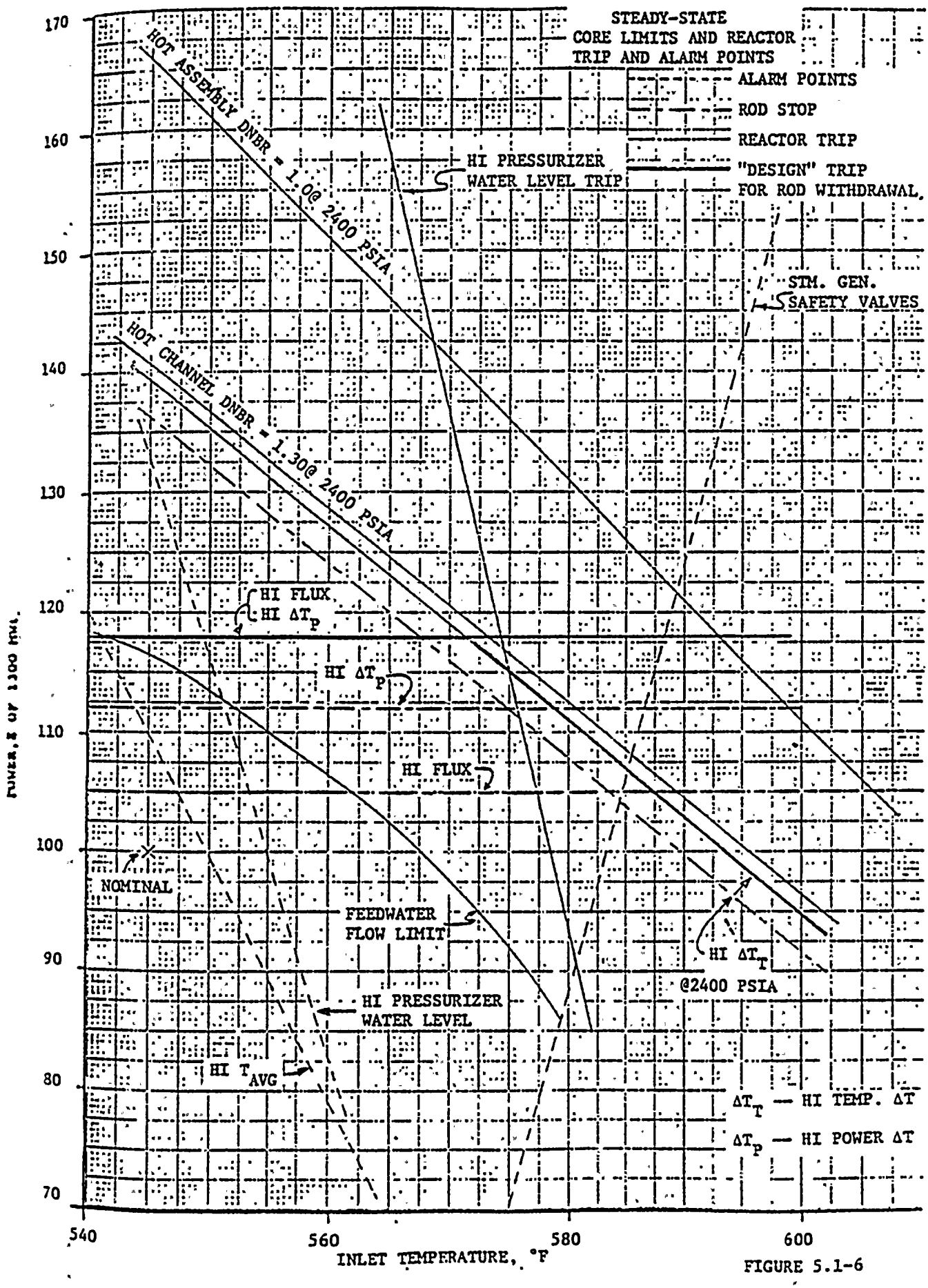
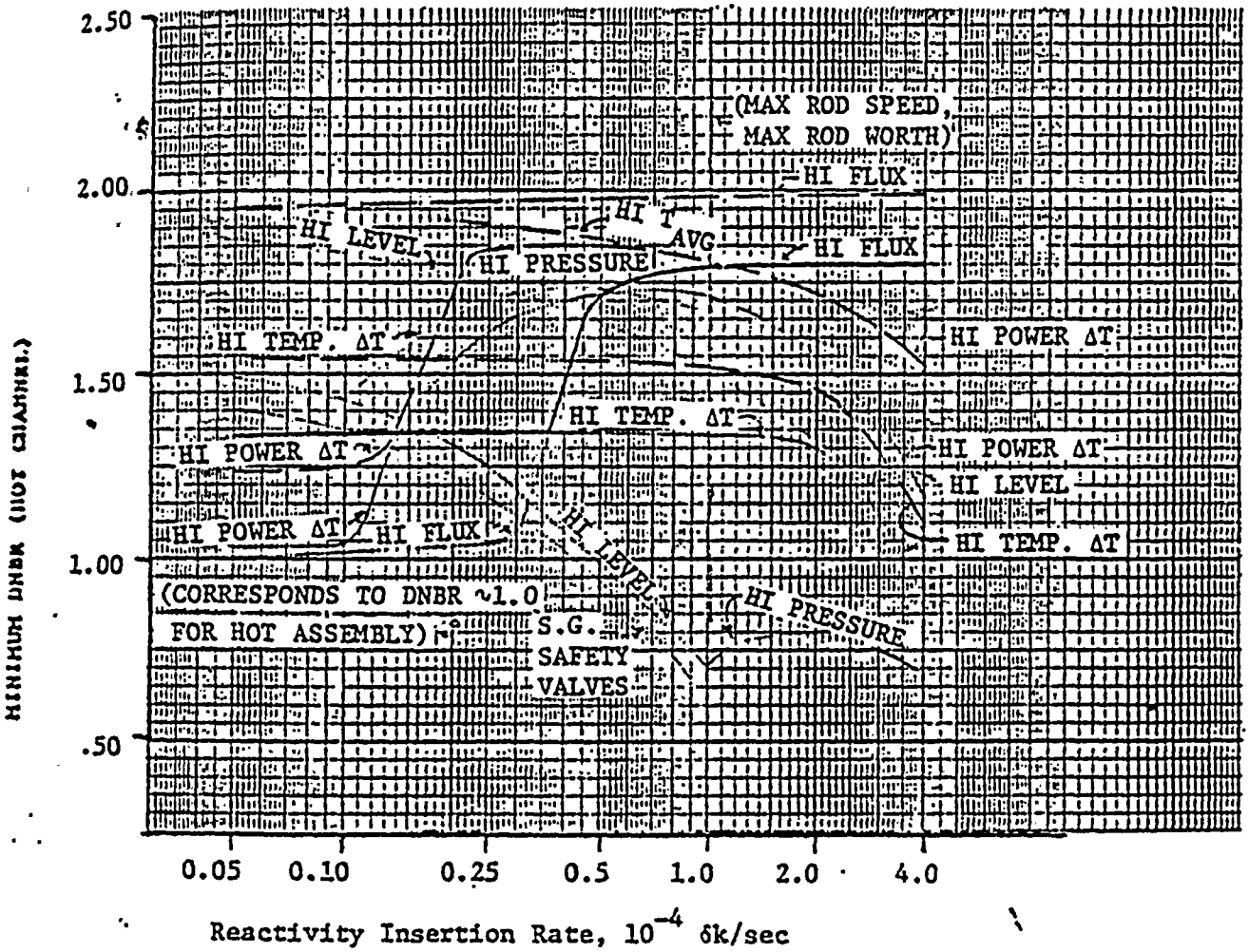

STEADY-STATE
CORE LIMITS AND REACTOR
TRIP AND ALARM POINTS
ALARM POINTS
ROD STOP
REACTOR TRIP
"DESIGN" TRIP
FOR ROD WITHDRAWAL.
HOT ASSEMBLY DNBR = 1.0@ 2400 PSIA
HOT CHANNEL DNBR = 1.30@ 2400 PSIA
HI PRESSURIZER
WATER LEVEL TRIP
STM. GEN.
SAFETY VALVES
HI FLUX
HI ΔT_P
HI ΔT_P
HI FLUX
NOMINAL
FEEDWATER
FLOW LIMIT
HI ΔT_T
@2400 PSIA
HI PRESSURIZER
WATER LEVEL
HI T_{AVG}
ΔT_T — HI TEMP. ΔT
ΔT_P — HI POWER ΔT
170
160
150
140
130
120
110
100
90
80
70
540
560
580
600
INLET TEMPERATURE, °F

FIGURE 5.1-6

BEGINNING OF LIFE ROD WITHDRAWAL FROM 102% POWER

MINIMUM DNBR



ALARM
ROD STOP
REACTOR TRIP
"DESIGN" REACTOR TRIP
CORE LIMIT

FIGURE 5.1-7

BEGINNING OF LIFE ROD WITHDRAWAL FROM 102% POWER
TIME OF EVENT

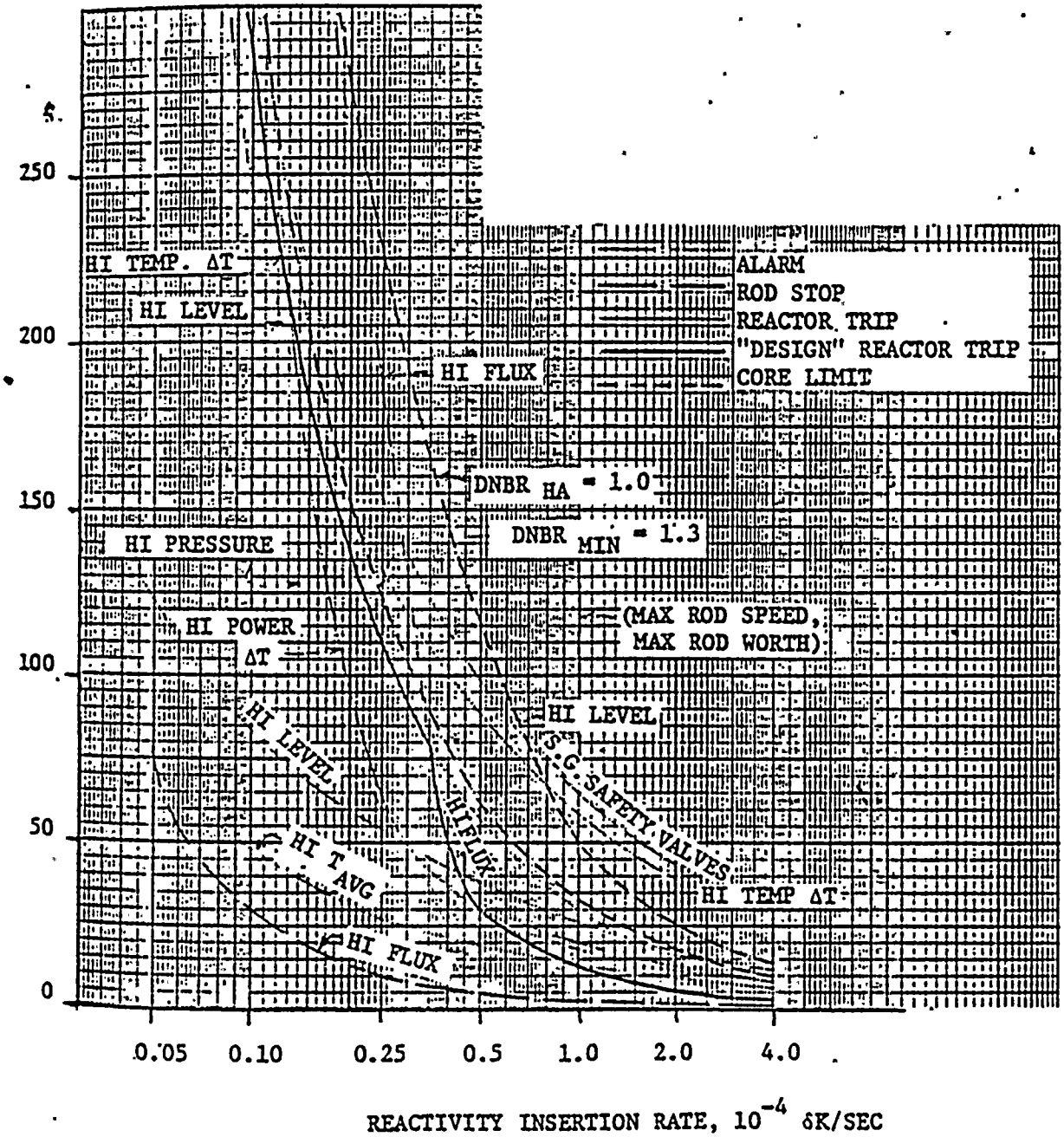
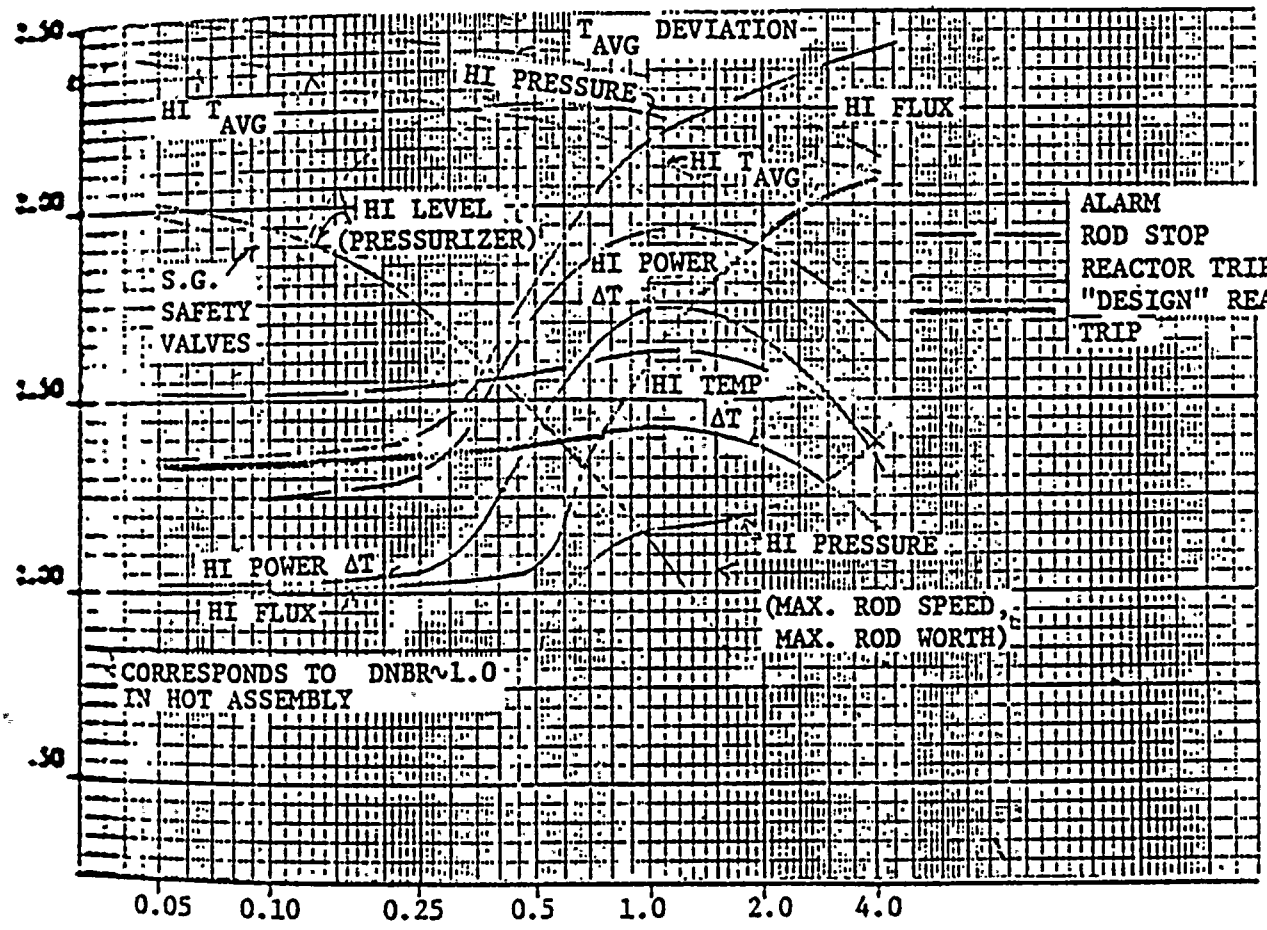


FIGURE 5.1-8

BEGINNING OF LIFE ROD WITHDRAWAL FROM 80% POWER

MINIMUM DNBR



REACTIVITY INSERTION RATE, 10^{-4} δK/SEC

FIGURE 5.1-9

BEGINNING OF LIFE ROD WITHDRAWAL FROM 80% POWER

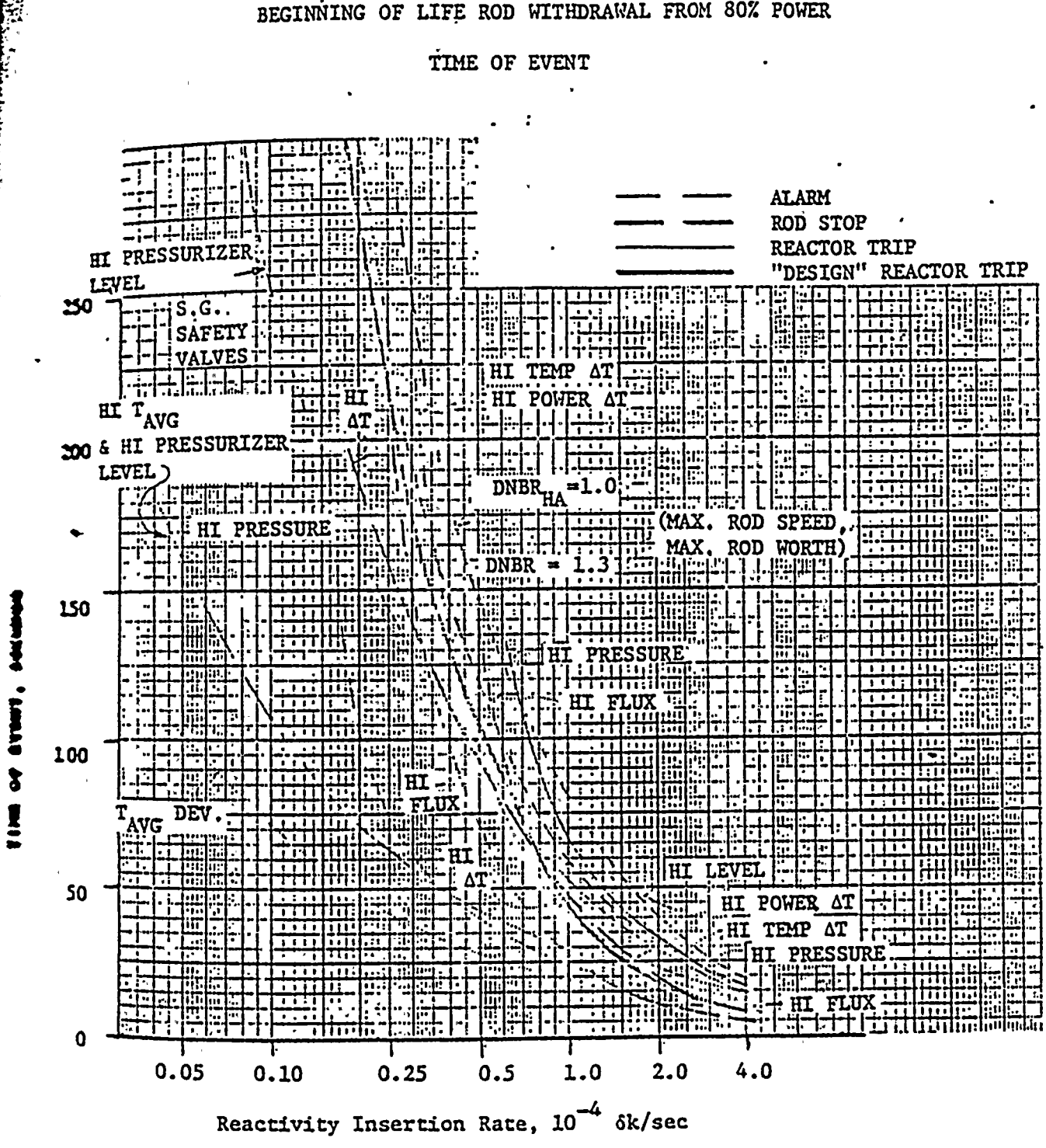


FIGURE 5.1-10

5.2 LOSS OF FEEDWATER

During power operation, loss of feedwater to the steam generators is of potential concern because it affects the ability of the steam generators to remove decay heat after trip. The protection for this accident consists of reactor trip and an auxiliary feedwater system.

This evaluation describes the Control and Protection System instrumentation provided on a typical Westinghouse PWR Plant to directly monitor or control steam generator water level. Loss of feedwater accidents without credit for this instrumentation are evaluated. Typical Westinghouse design requirements for the auxiliary feedwater system are included.

A typical 1456 MWt two-loop plant was selected for the transient analysis. A loss of feedwater accident to one steam generator is most severe on a two-loop plant. For a complete loss of feedwater, the transient is dependent on the normalized kinetic parameters; e.g., power per loop, so the results shown here are representative for all plants currently under design.

In all cases, diverse automatic reactor trips insure a plant trip before any core damage or system overpressure occurs. Manual actuation of the auxiliary feedwater system is considered an adequate backup to the automatic actuation. There is sufficient time (24 minutes) and alarms to take credit for manual actuation.

Interactions of steam generator level control and protection resulting from random failure modes are presented in Section 4.2.5. Alarms actuated

for a complete loss of feedwater accident are presented in Table 5.2-1. Fault trees for loss of feedwater accidents are presented in Figures 5.2-1, 5.2-2, and 5.2-3.

5.2.1 LOSS OF FEEDWATER - TRANSIENT ANALYSIS

Several representative transient cases are evaluated for loss of feedwater accidents. Figure 5.2-4 shows the transient resulting from complete loss of the steam flow control signal. As shown by the figure, the Level Control System restores water level such that only a temporary decrease in water level occurs. There is no approach to unsafe conditions or to any reactor trip set point.

Figures 5.2-5 and 5.2-6 illustrate a typical complete loss of feedwater to one steam generator of a two-loop plant. No credit was taken for reactor trips derived from the steam generator. The loss of subcooled feedwater is reflected to the reactor as a small decrease in thermal load, causing the increase in pressure and temperature shown in the first minute. (The reactor was assumed to be in manual control with no manual correction.) One minute after the loss of feedwater, the steam generator tubes begin to uncover, causing a rapid pressure and temperature increase. If maximum pressure control capacity (power operated relief valves) is available, the pressure rise is limited and a high pressure reactor trip does not result. A reactor trip on high pressurizer level occurs approximately two minutes after the loss of feedwater.

water inventory in the second steam generator is sufficient to bring the plant to normal no-load conditions. There is no overpressure or loss of water from the Reactor Coolant System.

Figures 5.2-7 and 5.2-8 illustrate a worst case complete loss of feedwater to all steam generators with no trip from steam generator instrumentation. A conservative evaluation is done for a high-power density plant typical of current PWR design (1456 MWt 2-loop). No credit is taken for charging systems or for energy absorption by metal in the Reactor Coolant System. The results are considered to be extreme values rather than realistic conditions for an actual plant.

The reactor trips on high pressurizer pressure about one minute after the loss of feed. Stored heat in the core continues to heat the reactor coolant and the pressurizer fills in about three minutes. Steam dump values open fully under T_{avg} control and reduce steam line pressure.

After about ten minutes, the Reactor Coolant System begins to boil, at which time the reactor coolant pumps are assumed to cease adding energy to the coolant. Boiling causes a rapid increase in the volumetric surge rate, and system pressure rises until the volumetric expansion is balanced by safety value capacity for water relief. (No credit was taken for the power-operated relief values in this analysis.)

Steam generated in the core is assumed to fill the upper reactor vessel, the steam generators, and half of the coolant piping before escaping to the pressurizer. During this four minute period, most of the reactor

coolant fluid is lost as water discharge through the pressurizer safety valve. As steam is discharge through the pressurizer, pressure decreases to the set pressure for the safety valves.

After an additional ten minutes of boiling, (24 minutes after the loss of feedwater), the top of the core is nearly uncovered. It was assumed that the Auxiliary Feedwater System was manually actuated at this time (push buttons on the control board) and 200 gpm auxiliary feedwater per steam generator began immediately. Within two minutes of starting auxiliary feedwater, the steam generator heat removal exceeds decay heat and reactor coolant temperature and pressure rapidly decrease.

5.2.2 TYPICAL SYSTEM DESIGN REQUIREMENTS

Auxiliary Feedwater System

To prevent release of reactor coolant through pressurizer safety valves and to protect the core, a supply of high pressure feedwater must be provided for the removal of residual heat from the core by heat exchange in the steam generators when the main feedwater pumps cease to operate on blackout or because of fault conditions.

Typical criteria for actuation of auxiliary feedwater is presented in Table 5.2-2.

A safety requirement is to include two separate auxiliary feedwater systems to ensure reliability of supply.

One system utilizes a steam turbine driven auxiliary feedwater pump, the turbine being connected such that steam can be supplied from some

or all of the steam generators. The flow rate, usually about 200 gpm per steam generator, is sufficient to maintain a minimum depth of water in the steam generators.

The other system utilizes two (2) reserve auxiliary feedwater pumps, each of about half the capacity of the steam driven pump. Flow rate is sufficient to ensure cooling of the system and to prevent water discharge from Reactor Coolant System relief valves. The reserve auxiliary feedwater pumps normally are driven by prime movers using a source of energy other than steam from steam generators.

The head generated by the feedwater pumps is to be sufficient to ensure that feedwater can be pumped into the steam generator when safety valves are discharging. Pumps are capable of starting and delivering feedwater within two (2) minutes of the blackout or fault conditions requiring pump actuation.

The typical design basis for sizing auxiliary feedwater pumps is given by Table 5.2-3.

Sources of water for auxiliary and reserve auxiliary feedwater pumps are duplicated or if convenient, triplicated. Ordinarily, water is drawn from a condensate storage tank containing water of normal purity, but may be drawn through emergency connections from other sources such as city water, well water, fire-main water, service water, etc., to obtain a supply under sufficient pressure to satisfy auxiliary feedwater pump suction requirements under emergency conditions.

feedwater from the auxiliary pumps is delivered to the steam generators through pipelines separate from the main feed pipelines. Pipelines are suitably spaced to assure that a single fault does not prevent feedwater flow. The whole of the auxiliary feedwater system (water supply, piping, pumps, diesel generators, etc.) must be "Class I" seismic design standard.*

Main Steam and Feedwater Piping

A failure of any main steam or feedwater line or malfunction of a valve installed therein or any consequential damage must not reduce flow capability of the auxiliary (emergency) feedwater system, render inoperable any engineered safeguard service (i.e., controls, electric cables, containment cooling piping, etc.), initiate a loss-of-coolant accident, cause failure of any other steam or feedwater line, result in the containment pressure exceeding the design value or impair its impermeability and integrity.

The steam and feedwater lines together with their supports and structures between each steam generator and their associated isolation valves are to be "Class I" seismic design standard.*

* The expression "Class I" used in this context is defined in "Design of Nuclear Power Reactors against Earthquakes" in a document entitled "Behaviour of Structures During Earthquakes" Appendix A, by J. W. Housner, Professor of Civil Engineering, California Institute of Technology. Pasadena, California. Published by American Society of Civil Engineers - Engineering Mechanics Division. (October 1959 EM4)

TABLE 5.2-1

ALARMS ACTUATED FOR A COMPLETE LOSS OF FEEDWATER ACCIDENT

1. Cause of fault (in general, any condition causing a complete loss of feedwater causes an alarm)
2. Low feedwater flow (partial reactor trip, two channels per steam generator)
3. Steam generator level deviation (one per steam generator)
4. Low steam generator level (partial reactor trip, in coincidence with 2. above, two channels per steam generator)
5. Low-low steam generator level (reactor trip, three channels per steam generator)
6. Automatic control rod motion
7. T_{avg} deviation
8. High T_{avg} (3 or 4 channels)
9. Pressurizer level deviation
10. High pressurizer pressure (two channels)
11. Pressurizer relief line high temperature
12. High pressurizer pressure reactor trip

    Note: It is assumed that the turbine and reactor are tripped on high pressurizer pressure.
13. Pressurizer safety valve outlet high temperature
14. High pressurizer level reactor trip
15. Low steam line pressure (not on all plants)
16. Pressurizer relief tank liquid high temperature
17. Pressurizer relief tank high pressure
18. Pressurizer relief tank high level
19. High containment pressure (safety injection actuation, at about 10% of design pressure)
20. Low pressurizer level (partial safety injection actuation)

TABLE 5.2-2

TYPICAL CRITERIA FOR AUXILIARY FEEDWATER ACTUATION

1. Motor-Driven Pumps

   a) Low-low level in any steam generator starts both pumps. This action requires the same bistables and relay logic as used for the reactor trip. (2/3 circuitry for any steam generator).

   b) Opening of both feedwater pump circuit breakers starts both pumps (1/1 + 1/1 logic).

   c) Safety injection sequence

   d) Manual.

2. Turbine-Driven Pump

   a) Low-low level in two steam generators. (Same circuitry as I.A. above)

   b) Loss of voltage on both 4KV buses (1/1 + 1/1 logic)

   c) Manual.

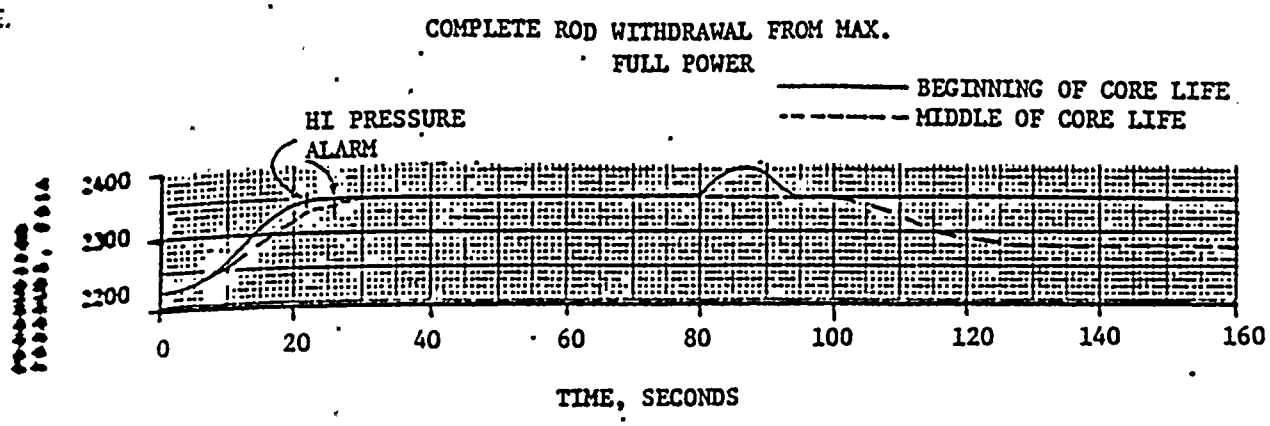
3. General Criteria

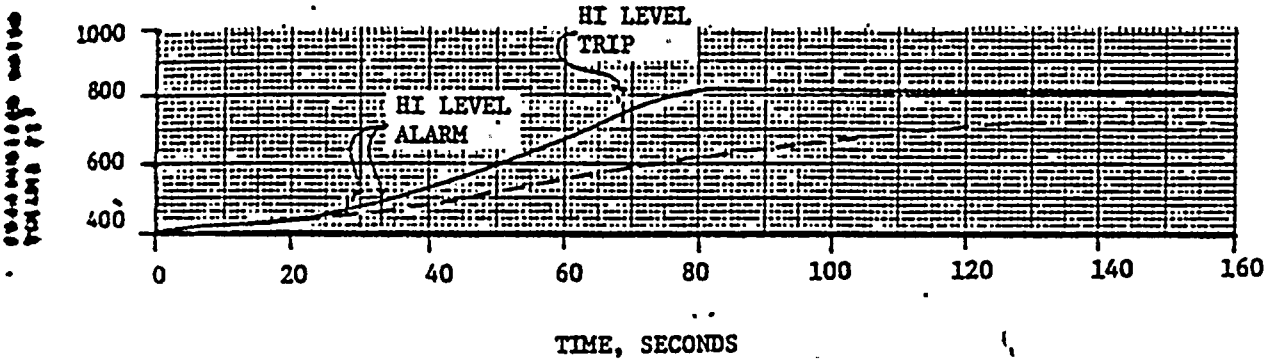
   a) All three pumps are to have independent starting circuits such that no single failure prevents more than one pump from starting.

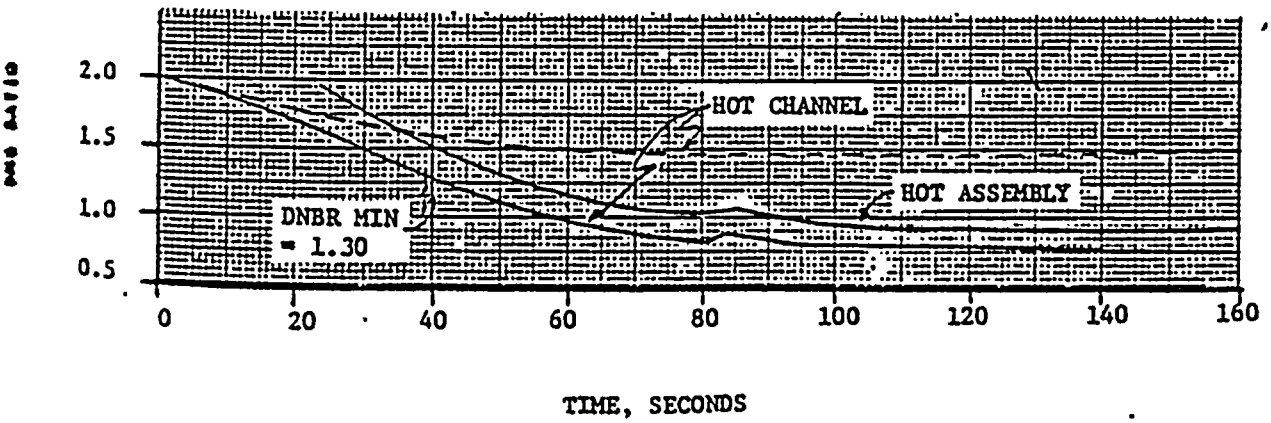
   b) Instrmentation and logic circuits for 1a and 2a must meet the single-failure criterion for actuation and be capable of testing at power. Compatibility with reactor trip circuit testing is also required.

   c) Spurious actuation due to unusual failures is tolerable, but routine testing of reactor trip circuits should not cause spurious starts.

COMPLETE ROD WITHDRAWAL FROM MAX.
FULL POWER







d) Instrumentation and logic for 1b and 2b should be considered as operational signals for economic (not public safety) protection, (Similar to reactor trip on reactor coolant pump circuit breaker opening).

e) As Engineered Safeguards components, the actuation circuitry for auxiliary feedwater actuation shall meet all applicable IEEE Design Criteria.

TABLE 5.2-3

TYPICAL DESIGN BASIS FOR SIZING AUXILIARY FEEDWATER PUMPS

1. STEAM-DRIVEN PUMPS

The steam-driven pump capacity is adequate to maintain at least 10 feet of water in all steam generators in the event of loss of station power from normal full power operation. No credit is allowed for motor-driven pump capacity.

2. MOTOR-DRIVEN PUMPS

Each motor-driven pump, by itself, is adequate to prevent water relief from the pressurizer relief valves under the following assumptions:

a) Plant trip occurs from maximum steady-state power and temperature conditions.

b) All steam generators are at their low-low level trip points at the time of trip.

c) No credit is taken for any additional sources of feedwater after trip (station blackout assumed.)

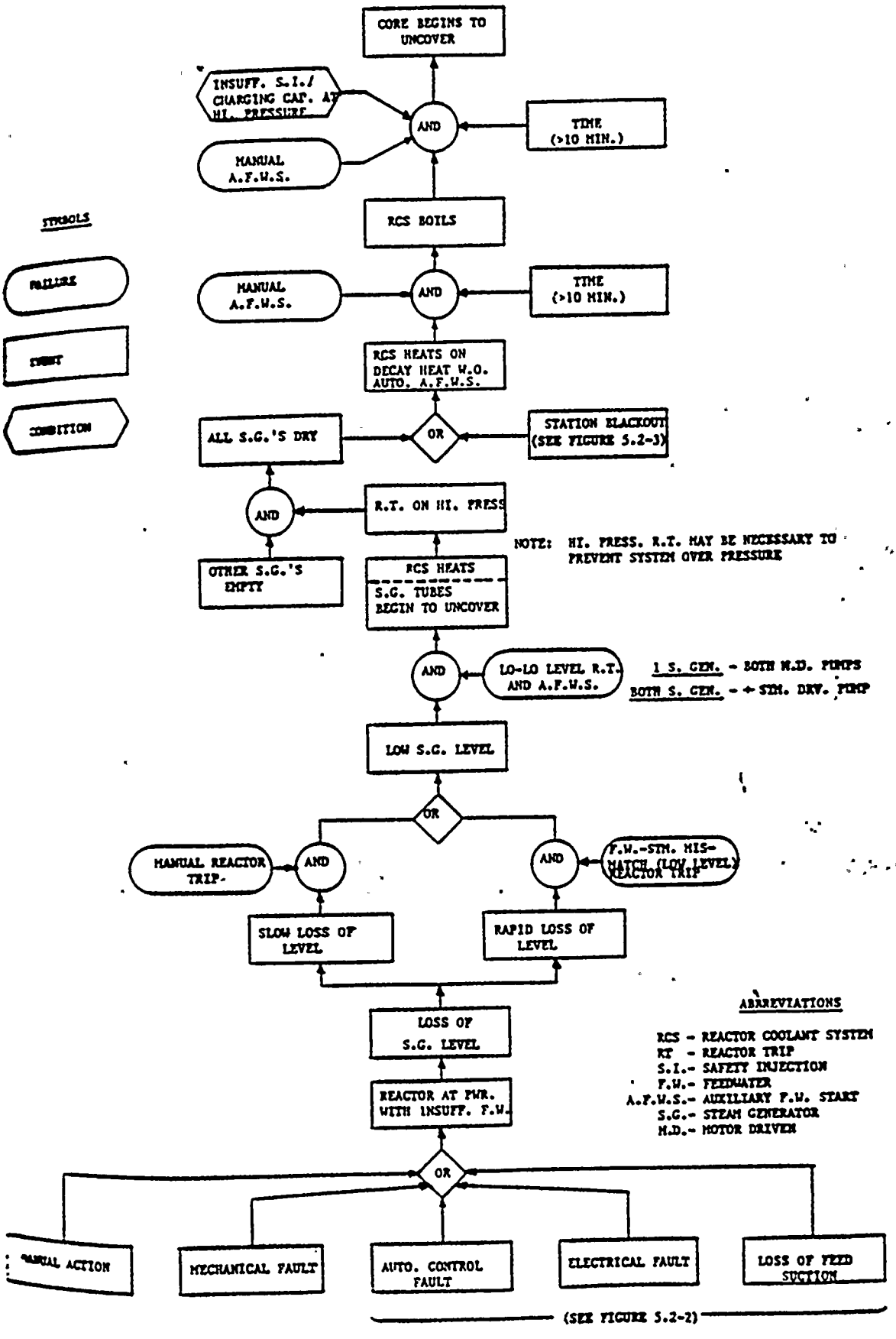
d) At least half, but not all, of the steam generators are supplied with auxiliary feedwater.

e) Natural circulation exists in the Reactor Coolant System.

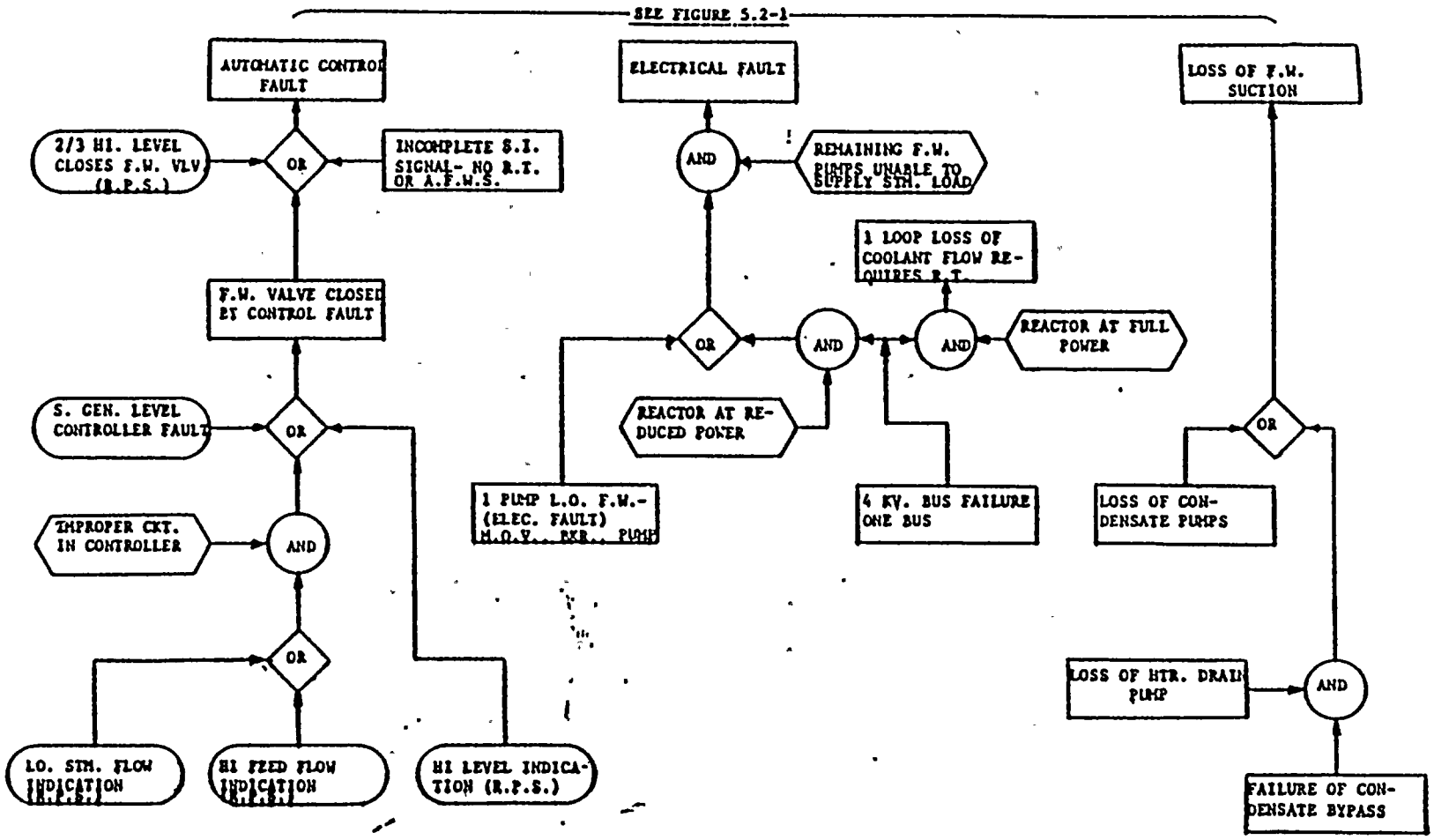
f) No credit is taken for charging or letdown from the Reactor Coolant System.

g) Applicable starting delays and feedwater pipe purging times are used.

FAULT TREE FOR LOSS OF FEEDWATER FLOW



FAULT TREE FOR LOSS OF FEEDWATER FLOW



SYMBOLS

FAILURE

EVENT

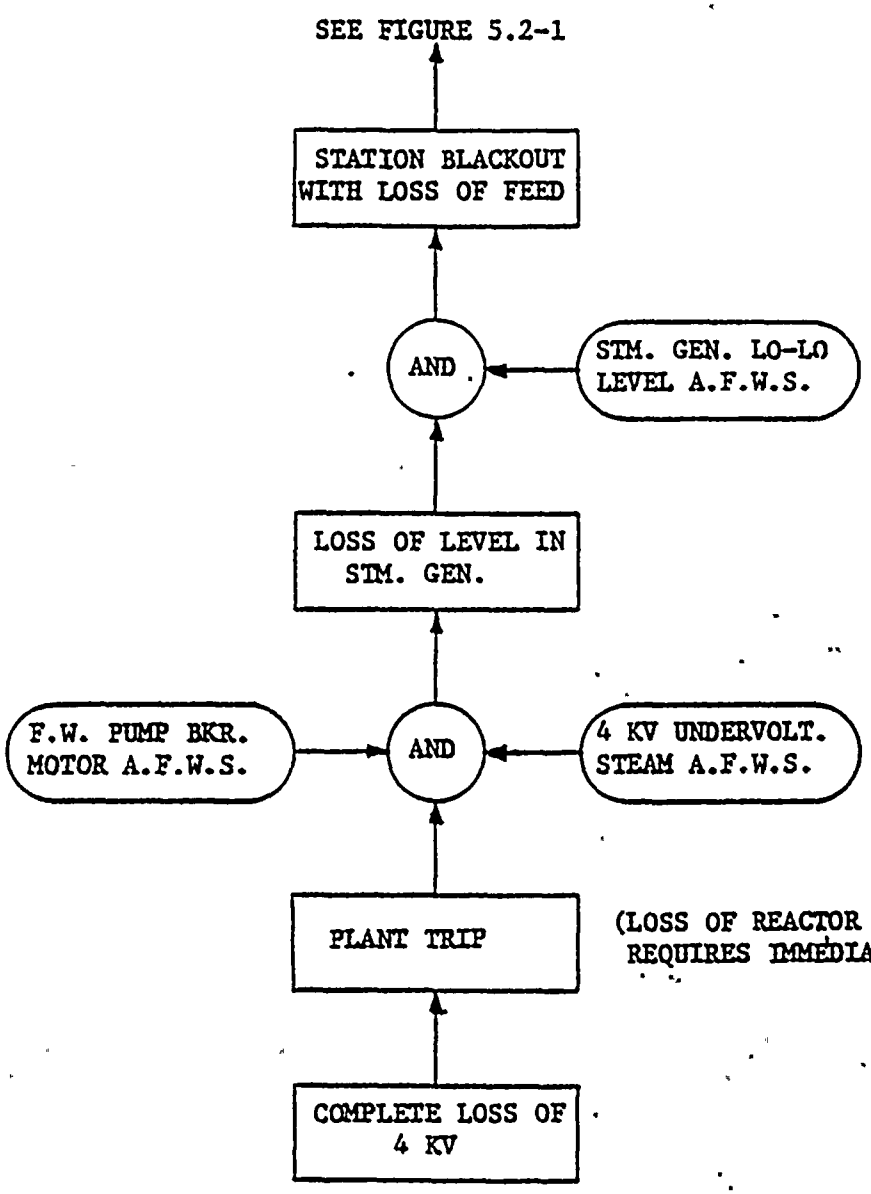
CONDITION

ABBREVIATIONS

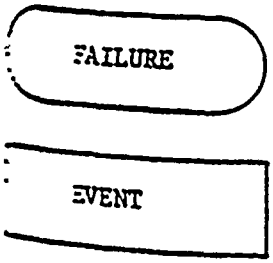
R.T. - REACTOR TRIP
S.I. - SAFETY INJECTION
R.P.S. - REACTOR PROTECTION SYSTEM
F.W. - FEEDWATER
A.F.W.S. - AUXILIARY F.W. START

FIGURE 5.2-2

FAULT TREE FOR LOSS OF FEEDWATER FLOW



SYMBOLS

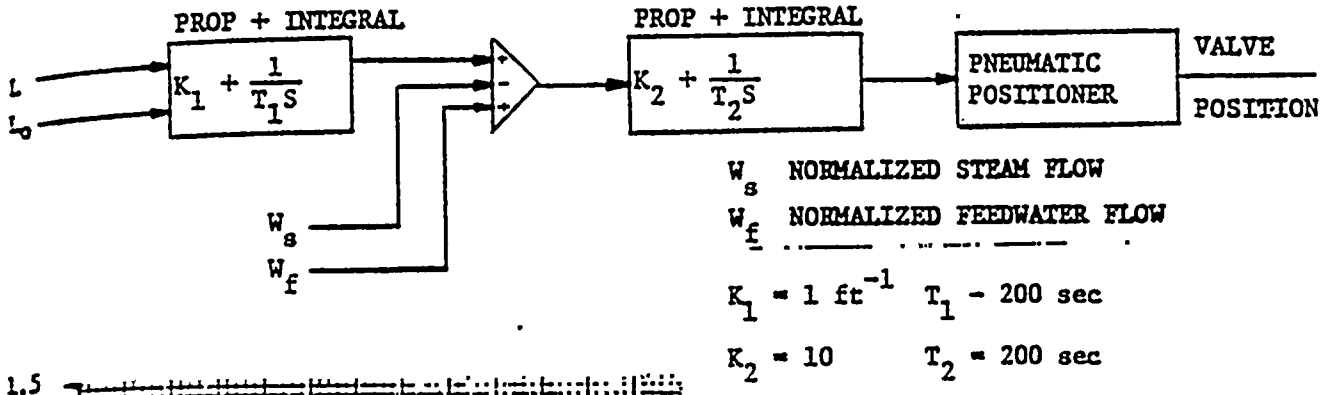


ABBREVIATIONS

F.W. - FEED WATER
A.F.W.S. - AUXILIARY F.W. START

FIGURE 5.2-3

LEVEL RESPONSE TO LOSS OF STEAM FLOW SIGNAL



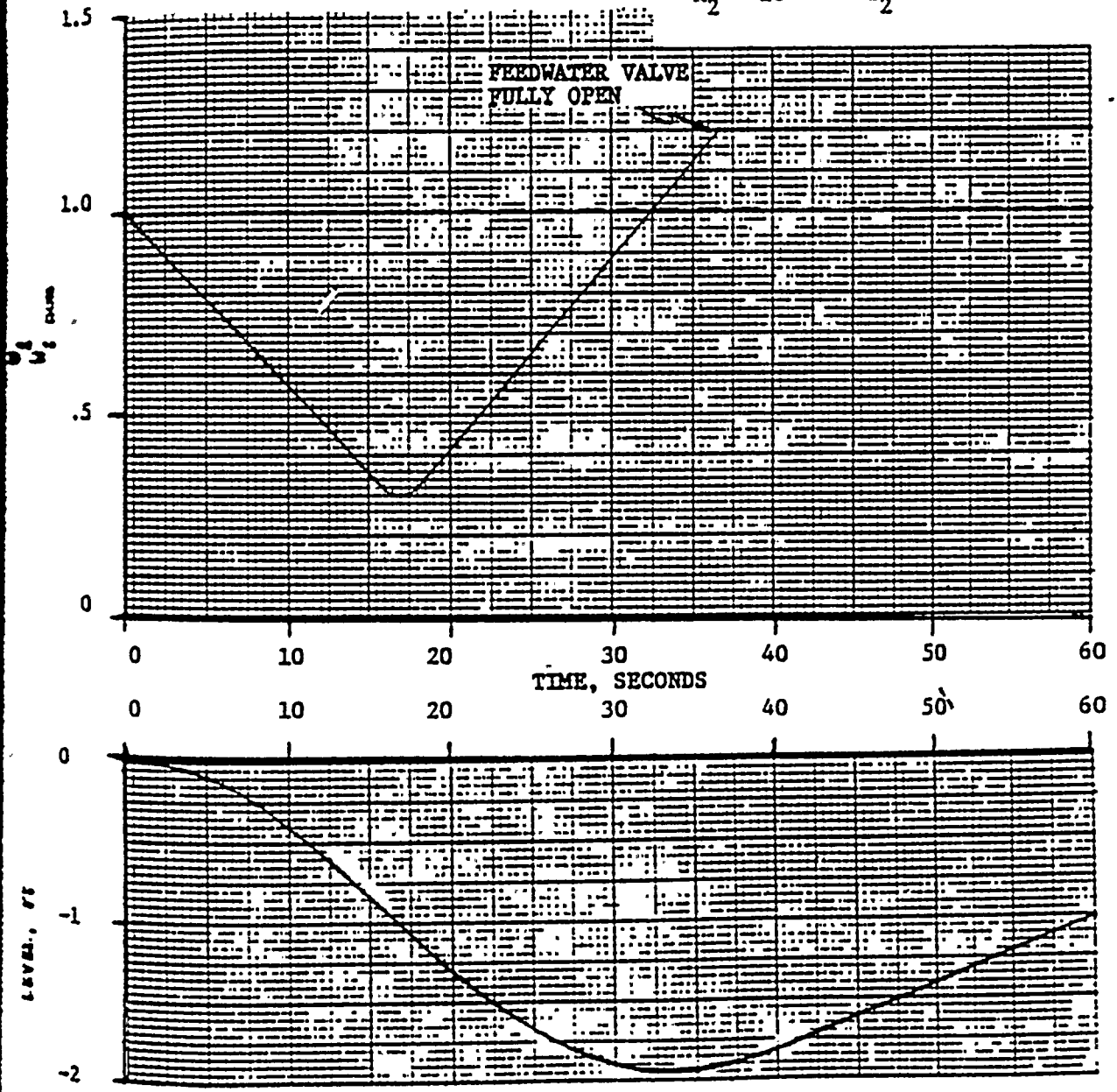


FIGURE 5.2-4

LOSS OF FEEDWATER TO ONE STEAM GENERATOR AT
T = ONE SECOND

TYPICAL TWO-LOOP PLANT

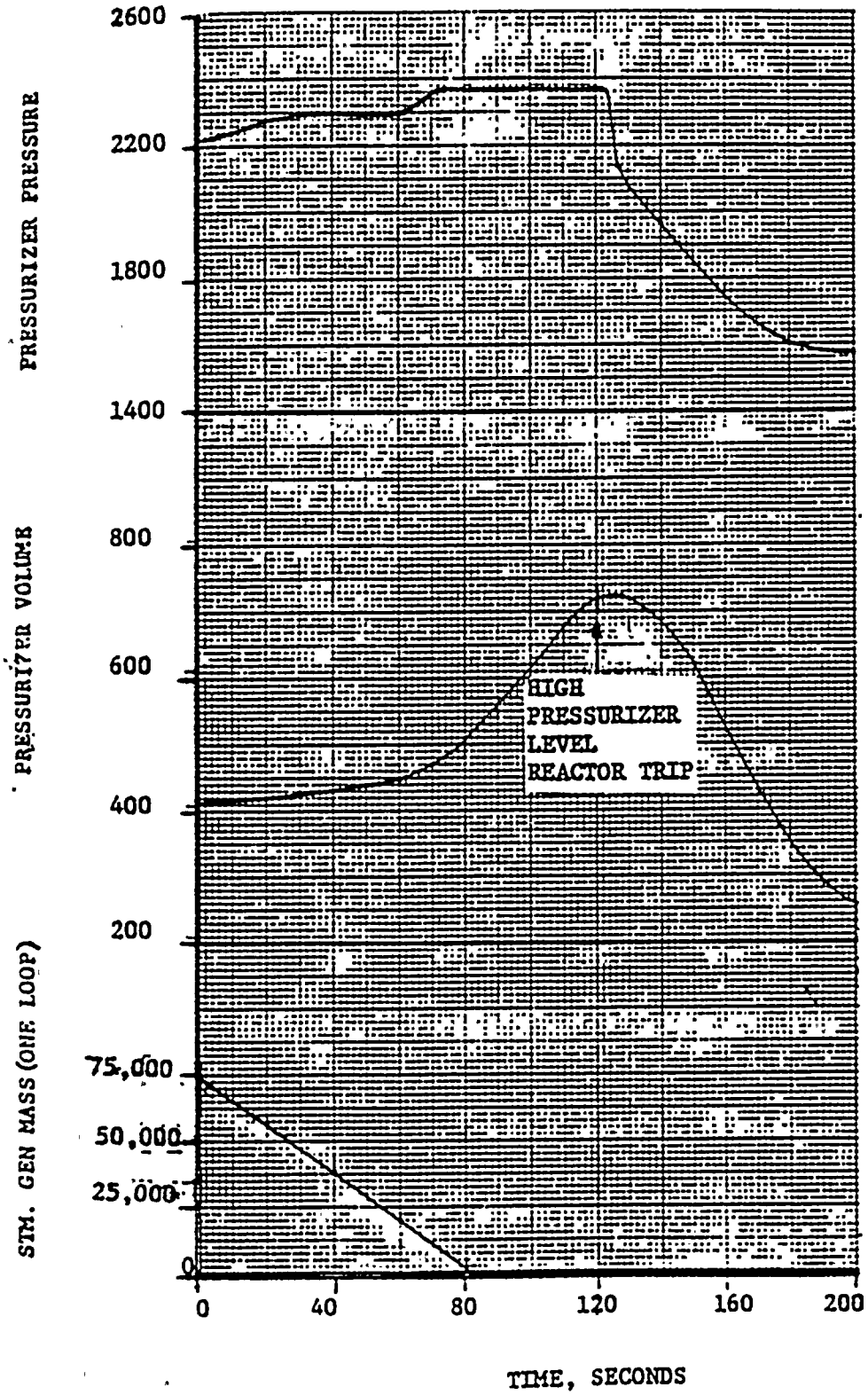


FIGURE 5.2-5

LOSS OF FEEDWATER TO ONE STEAM GENERATOR AT T = ONE SECOND

TYPICAL TWO-LOOP PLANT

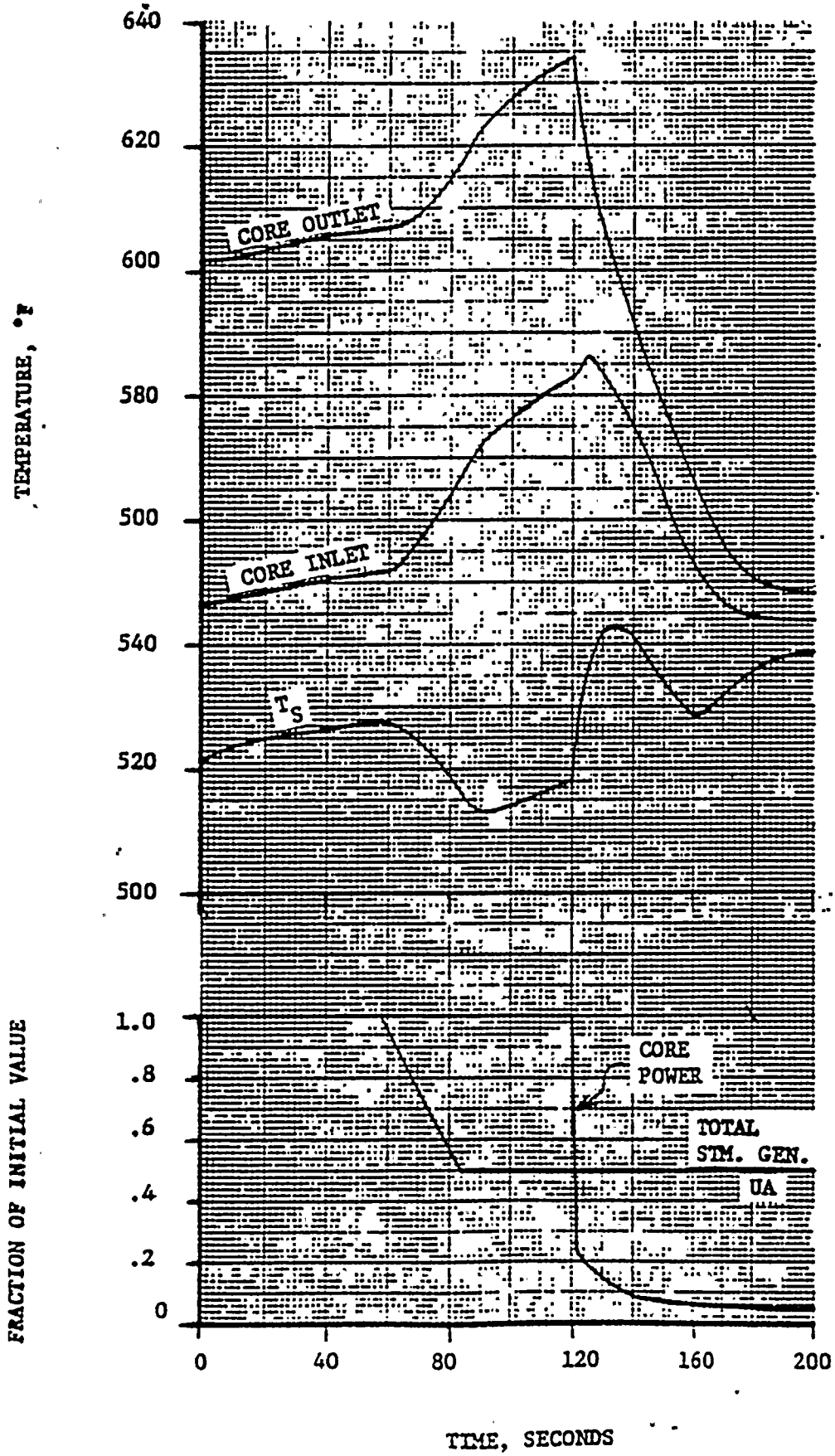


FIGURE 5.2-6

COMPLETE LOSS OF FEEDWATER

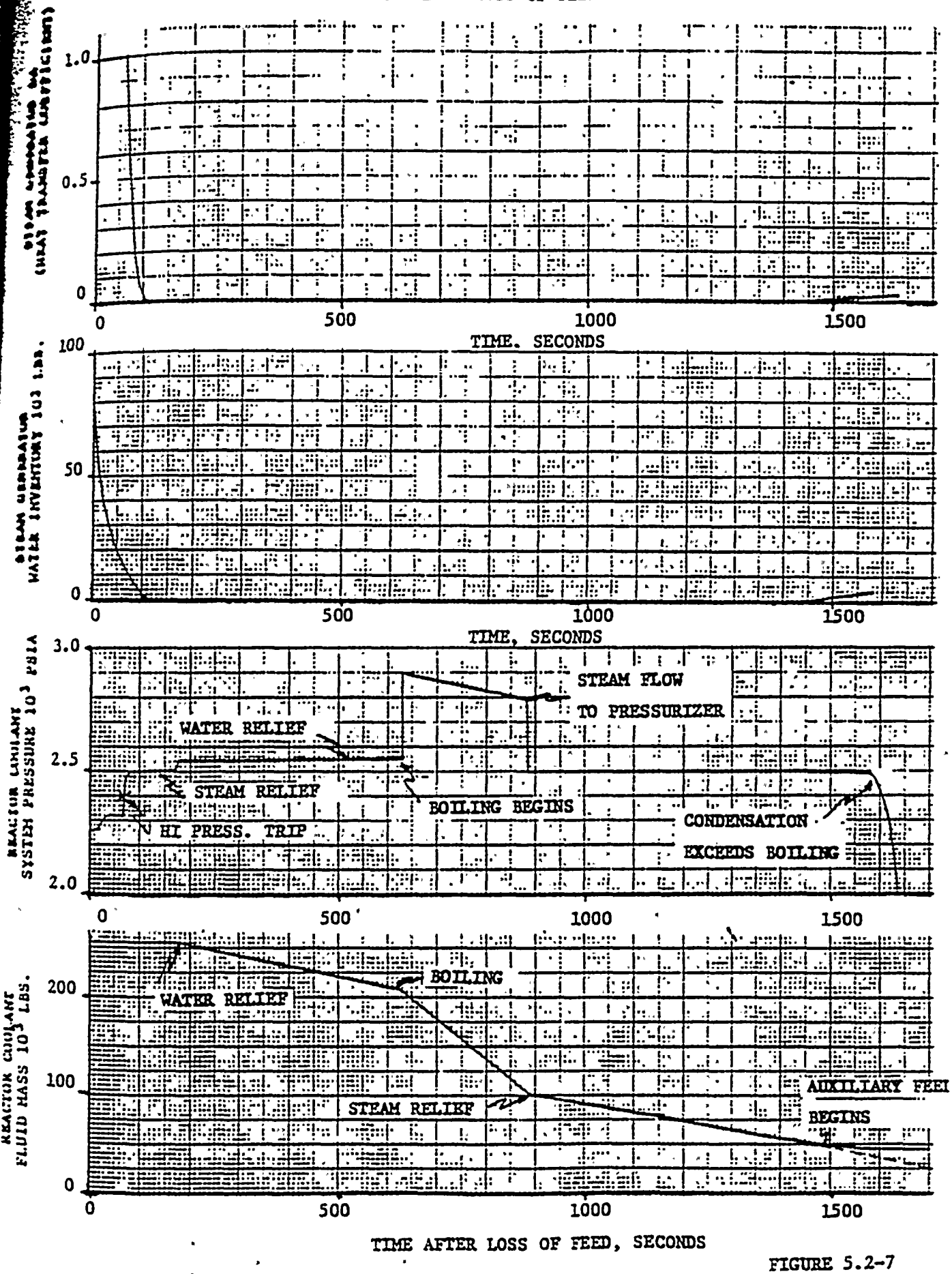
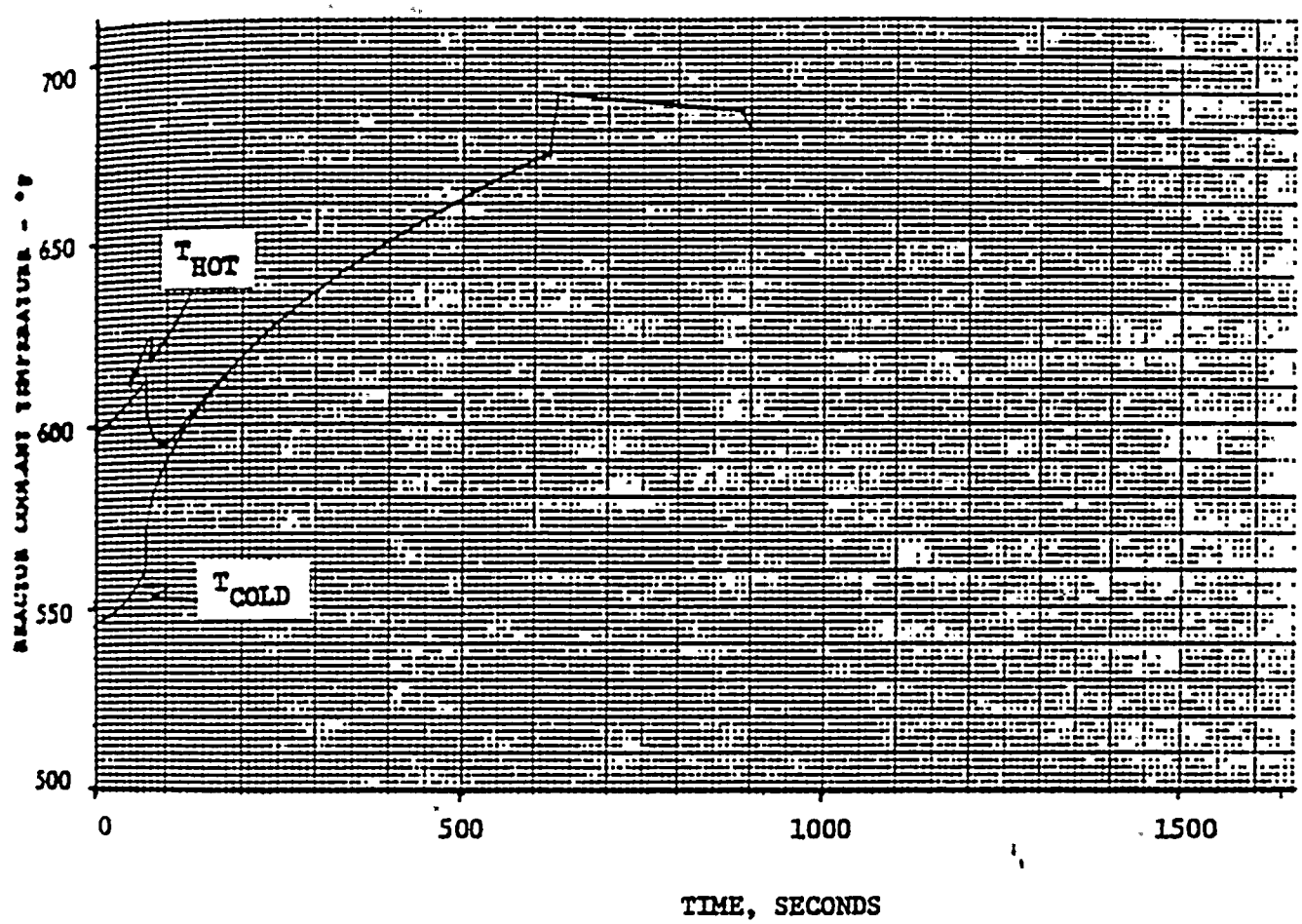


FIGURE 5.2-7

COMPLETE LOSS OF FEEDWATER



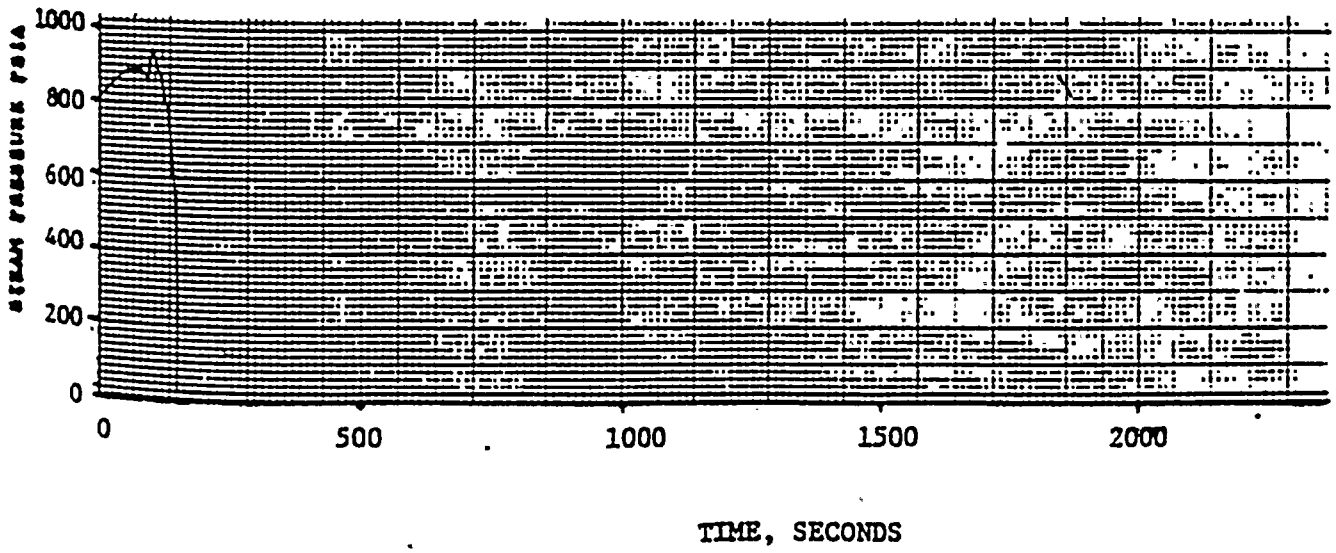


FIGURE 5.2-8

AUXILIARY FEEDWATER SYSTEM SCHEMATIC

2 LOOP PLANT

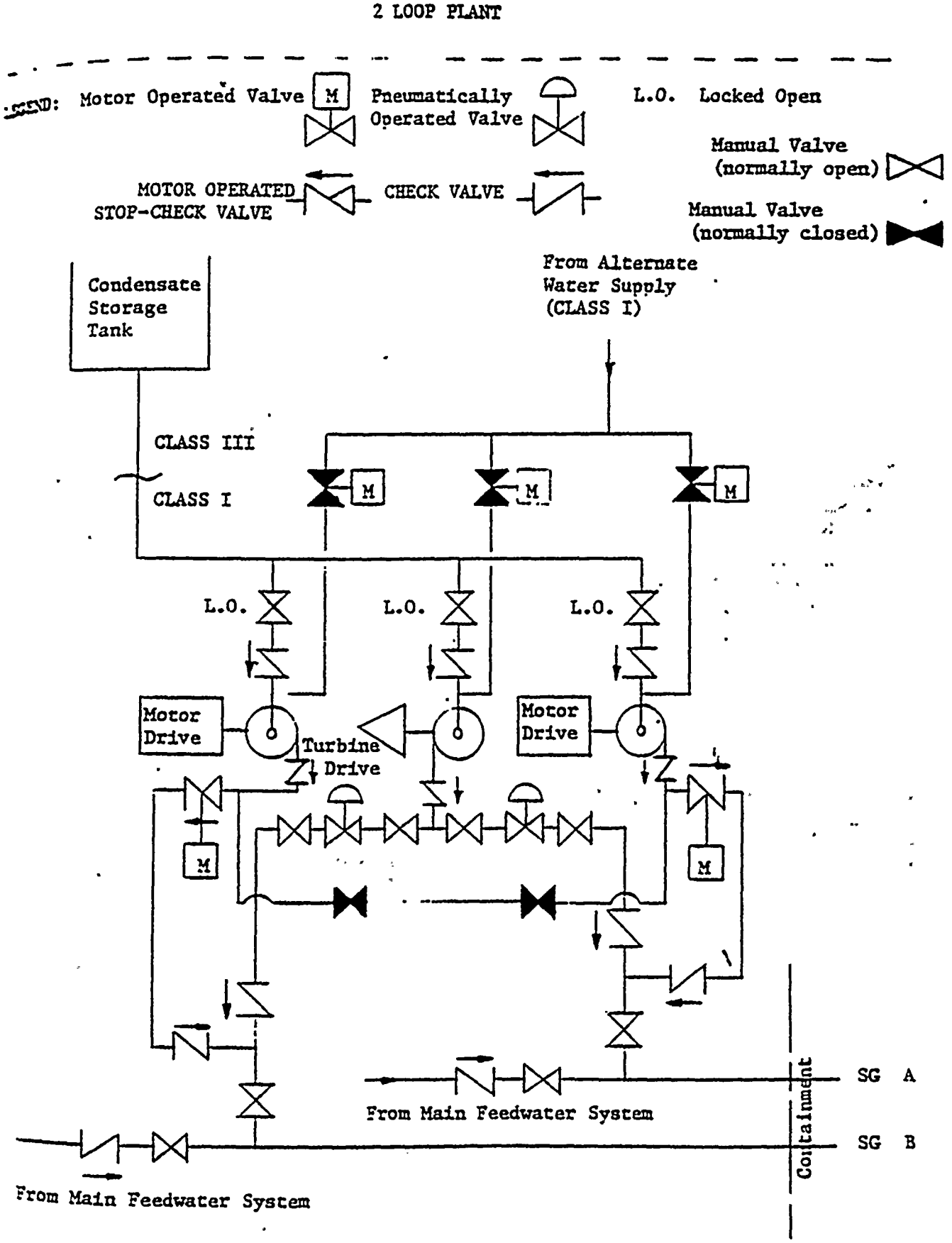


FIGURE 5.2-9

5.3 LOSS OF COOLANT FLOW ANALYSIS

5.3.1 INTRODUCTION AND SUMMARY

When the reactor is in the power range of operation, loss of coolant flow is of potential concern. Without sufficient flow, DNB and clad failure would quickly occur.

In Westinghouse PWR's, constant-speed pumps supply coolant flow. Flow is not regulated or otherwise varied. High-inertia flywheels are mounted on each pump so that flow decreases over a period of time (typically 12 seconds to half flow) following a loss of power to the pump motor. This flow coast-down allows for Protection System time delays and removal of stored heat in the fuel. Subsequent decay heat is removed by natural circulation.

Diverse, redundant protection circuits are provided to protect against all possible loss of flow accidents. These protection circuits are evaluated in this report for multiloop loss of flow, single loop loss of flow, and hypothetical pump seizure. Although design limits might be exceeded, the consequences are found to be tolerable in all cases even if any one protection circuit failed to perform its function.

5.3.2 PROTECTION SYSTEM DESCRIPTION

Numerous reactor trip circuits provide core protection for a loss of flow accident. These trips are:

a) Low reactor coolant flow,
b) Reactor coolant pump bus low voltage,
c) Reactor coolant pump bus low frequency,
d) Reactor coolant pump breaker position,
e) Overpower Delta-T.

Except for the overpower Delta-T trip, all trips are blocked below 10% power.

Low Reactor Coolant Flow

Three redundant flow channels are provided for each loop. At high power, loss of flow in any loop, as sensed by two of the three channels, actuates a reactor trip. The set point for this trip is typically at 90% of normal indicated flow.

At lower power (typically 50%, 65%, and 75% for 2, 3, and 4-loop plants respectively) loss of flow in any two loops actuates trip. The same flow set point and 2/3 logic is used as for the single loop low flow trip.

Reactor Coolant Pump Low Voltage

In order to insure that total loss of pump power does not violate the core design limits, a reactor trip is actuated by low voltage on the reactor coolant pump buses. The design requirement is to meet the single-failure criterion for complete loss of pump power. The trip logic is generally such that loss of power on any two buses causes a reactor trip.

Typical set points for this trip are in the range of 60% to 80% of normal voltage.

Reactor Coolant Pump Low Frequency

The reactor coolant pumps are provided with flywheels to increase their rotating inertia. This provides forced circulation for some period of time after a loss of power. It is conceivable that a rapid system frequency decrease would slow the pumps down faster than for a loss of power.

Therefore, an underfrequency reactor tirp is provided. The trip logic is identical to that used for the undervoltage reactor trip. In addition to tripping the reactor, underfrequency also trips open the reactor coolant pump circuit breakers to maintain effective flywheel inertia.

Typical setpoints for this trip are in the range of 56 - 58 cps.

Pump Circuit Breaker Position

A reactor trip derived from auxiliary contacts on the reactor coolant pump circuit breaker affords additional safety margin for the most likely causes of loss of flow. Trip logic is similar to that used for the low flow trip; i.e., opening of any breaker, as indicated by a position contact, actuates a reactor trip at high power, and opening of any two breakers at reduced power actuates a trip.

Overpower Delta-T Reactor Trip

This trip circuit is designed to protect the core against overpower transients. However, since Delta-T increases as flow decreases, it also provides backup protection for loss of flow accidents. On a two-loop plant, two Delta-T channels per loop are provided; one channel per loop is provided on three- and four-loop plants. For all plants, trip of two channels trips the reactor. During steady-state operation, the trip setpoint for these channels is in the range of 110% to 120% of the normal Delta-T indicated at full power. This setpoint is automatically reduced for increasing temperature (rate of change of T_{avg}) to compensate for piping delays. (However, the setpoint is not increased for decreasing T_{avg}.) Since T_{avg} also increases following a loss of flow accident, the Delta-T set-

point decreases at the same time as Delta-T increases. This significantly decreases the trip delay time.

Interlocks

Except for the overpower Delta-T reactor trip, the loss of flow protection trips are blocked at low power. This interlock is in itself redundant and diverse, in that the trip signal is passed if either 2/4 nuclear channels indicate above 10% or if 2/2 turbine load signals indicate above 10%.

Single loop loss of flow trips from low flow and circuit breaker position are blocked at reduced power. (The trip is passed if 2/4 nuclear channels indicate above a preset power.) Since these two trips share a common, non-diverse interlock, they should not be considered as completely diverse protection functions.

5.3.3 MULTILOOP LOSS OF FLOW

A fault tree for a multi-loop loss of flow accident is shown on Figure 5.3-1. Only electrical faults can cause all pumps to fail simultaneously, and the undervoltage and underfrequency reactor trips provide direct protection against these faults. The low flow reactor trip circuits provide backup protection for this accident, and they do not necessarily insure a minimum DNB ratio greater than 1.30.

Figure 5.3-4 illustrates the transient resulting from a complete loss of flow accident representative of high power density plants currently under design. The solid lines represent the design case, with reactor trip on undervoltage. The dashed lines illustrate the calculated transient if this reactor trip is neglected.

These calculations are done by standard design methods, with the usual assumptions for safety analysis; e.g., the most adverse steady-state operating conditions at the time of trip.

The accident is relatively rapid, with a DNB ratio of 1.3 in the hot channel reached in about two seconds. It is not appropriate, therefore, to assume any manual corrective action. Also, the minimum DNB ratio is reached at the time the hot spot heat flux begins to decrease. There is little transient overshoot except for reactor trip time delays.

The undervoltage trip is the design protection for this accident, and it meets the requirement that the minimum DNB ratio does not fall below 1.30. Less restrictive requirements would be imposed on a backup trip. A minimum allowable DNB ratio of 1.0 in the hot assembly could be selected on the basis that this would insure that core damage, if it occurred at all, would be limited to a very small fraction of the core. (The peaking factors in the hot assembly are essentially those in the hot channel without allowance for engineering subfactors.) Alternately, a hot-spot clad melting limit could be imposed for this accident on the backup protection. With either requirement, Protection System diversity exists.

The low flow reactor trip point is reached at 1.8 seconds, assuming a 3% error in the set point (trip point at 87% flow). Although the hot channel minimum DNB ratio is somewhat below 1.3, the hot assembly minimum DNB ratio is still well above 1.0. If DNB should occur at the hot spot, the transition boiling correlation indicates that peak clad temperature would be in the neighborhood of 1000°F, and no clad damage is expected. (See results for single loop loss of flow.)

The Delta-T transient is calculated for this case. Because of piping and instrument delays, a trip signal would not be generated until about 4 seconds after the loss of flow. The effect of rate compensation on T_{avg} is to reduce the trip set point. Even with this longer trip delay, the peak clad temperature is not expected to exceed 1500°F, well below the melting point. Therefore, three levels of protection exist for a multiloop loss of flow accident.

5.3.4 SINGLE LOOP LOSS OF FLOW

A fault tree for a single loop loss of flow accident is shown on Figure 5.3-2. Note that loss of power to one bus is the only credible way this accident can occur without an immediate trip from the pump circuit breaker. (An open circuit in the pump motor is a highly unlikely fault, and is shown for the sake of completeness.) The circuit breaker trip is therefore classed as a backup, or anticipatory, trip.

Figure 5.3-5 illustrates the transient resulting from a single-loop loss of flow accident in a high-power density, two-loop plant. The transient is less severe in a three or four-loop plant.

The low-flow reactor trip is the design protection for this accident, and it meets the design requirement of minimum hot channel DNB ratio no less than 1.30.

If the accident is caused by loss of bus voltage, and no credit is taken for the low flow reactor trip, the hot channel DNB ratio would be less than 1.3. However, a reactor trip on high Delta-T would terminate the

accident before DNB occurs in a significant percentage of the core. Assuming that the hot spot goes into DNB at the time the hot spot DNB ratio is 1.30, and assigning a conservative additional instrument delay of 0.9 sec. to the Delta-T trip, a peak hot spot clad temperature (on the inner clad surface) of approximately 1300°F is calculated using a transition boiling correlation.

Only the Delta-T transient for the active loop is shown on Figure 5.3-5. For the dead loop, Delta-T increases somewhat more rapidly. On a two-loop plant, two Delta-T channels exist on each loop, so a reactor trip is expected earlier than is shown.

In summary: For a single loop loss of flow accident, Protection System diversity does exist. At least two, and generally three, independent levels of protection exist.

5.3.5 LOCKED ROTOR ACCIDENT

The hypothetical case of an instantaneous pump seizure has been evaluated to determine whether diversity exists. The fault tree is shown on Figure 5.3-3.

If this accident occurs when the reactor is at high power, the core design limits are exceeded independent of any protective action. The design requirement for this accident is to prevent any consequential failure of the Reactor Coolant System. Failure could be caused by high system pressure. Also, systems calculations cannot be done with confidence if gross core damage occurs. For this reason, core conditions are evaluated.

The transient for a hypothetical locked rotor accident is shown on Figure 5.3-6. Flow through the Reactor Coolant System is rapidly reduced, leading to a reactor trip on a low-flow signal. Following the trip, heat stored in the fuel rods continues to pass into the core coolant, causing the coolant to expand. At the same time, heat transfer to the shell side of the steam generator is reduced, first because the reduced flow results in a decreased tube side film coefficient and then because the reactor coolant in the tubes cools down while the shell side temperature increases (turbine steam flow is reduced to zero upon plant trip). The rapid expansion of the coolant in the reactor core, combined with the reduced heat transfer in the steam generator, causes an insurge into the pressurizer and a pressure increase throughout the Reactor Coolant System. The insurge into the pressurizer compresses the steam volume, actuates the automatic Spray System, opens the power-operated relief valves, and opens the pressurizer safety valves, in that sequence. The two power-operated relief valves are designed for reliable operation and would be expected to function properly during the accident. However, for conservatism, their pressure-reducing effect is not included in the analysis.

With no protection, a peak reactor coolant pressure of approximately 3050 psia would be reached about 3.5 seconds after the pump seizes. After this time, fluid mixing and increased heat transfer in the active steam generator tend to reduce the pressurizer surge rate, and the pressurizer safety valves reduce pressure. (During the peak, the pressurizer surge rate may slightly exceed the pressurizer safety valve capacity, but pressurizer pressure does not significantly exceed the safety valve set

pressure plus allowance for accumulation.) Although the normal code-allowable pressure of 2750 psia is exceeded for this accident, the peak pressure is below the ultimate strength of all members of the Reactor Coolant System by an approximate factor of two. Therefore, the Reactor Coolant System would remain intact.

In the core, clad melting at the hot spot inner clad surface begins at 24 seconds. After this time, system calculations are uncertain.

The reactor trip set point for the redundant low flow instrumentation on the affected loop is reached within 0.1 seconds. Assuming DNB at 0.1 seconds, and a conservative trip delay (2 seconds before the nuclear flux is reduced to 80%), the peak clad temperature is approximately 1550°F and is reached at 4.5 seconds. Other calculated results for this case are peak system pressure of 2800 psia and less than 20% of the fuel rods with a calculated DNB ratio of 1.0 or less.

Neglecting this trip, a high pressurizer pressure trip point would be reached at about 1.5 seconds, and a high Delta-T trip (from the active loop) would be reached at about 4.5 seconds. The peak clad temperature for these cases would be 1750° and 1950° for the high pressure and high Delta-T trips respectively. Since these values are well below the melting point, no gross clad failure is expected.

In summary: For the hypothetical locked rotor accident, core design limits may be exceeded. However, three independent, diverse levels of protection exist, any of which would insure that the Reactor Coolant System boundary is not violated.

FAULT TREE FOR MULTILOOP LOSS OF FLOW

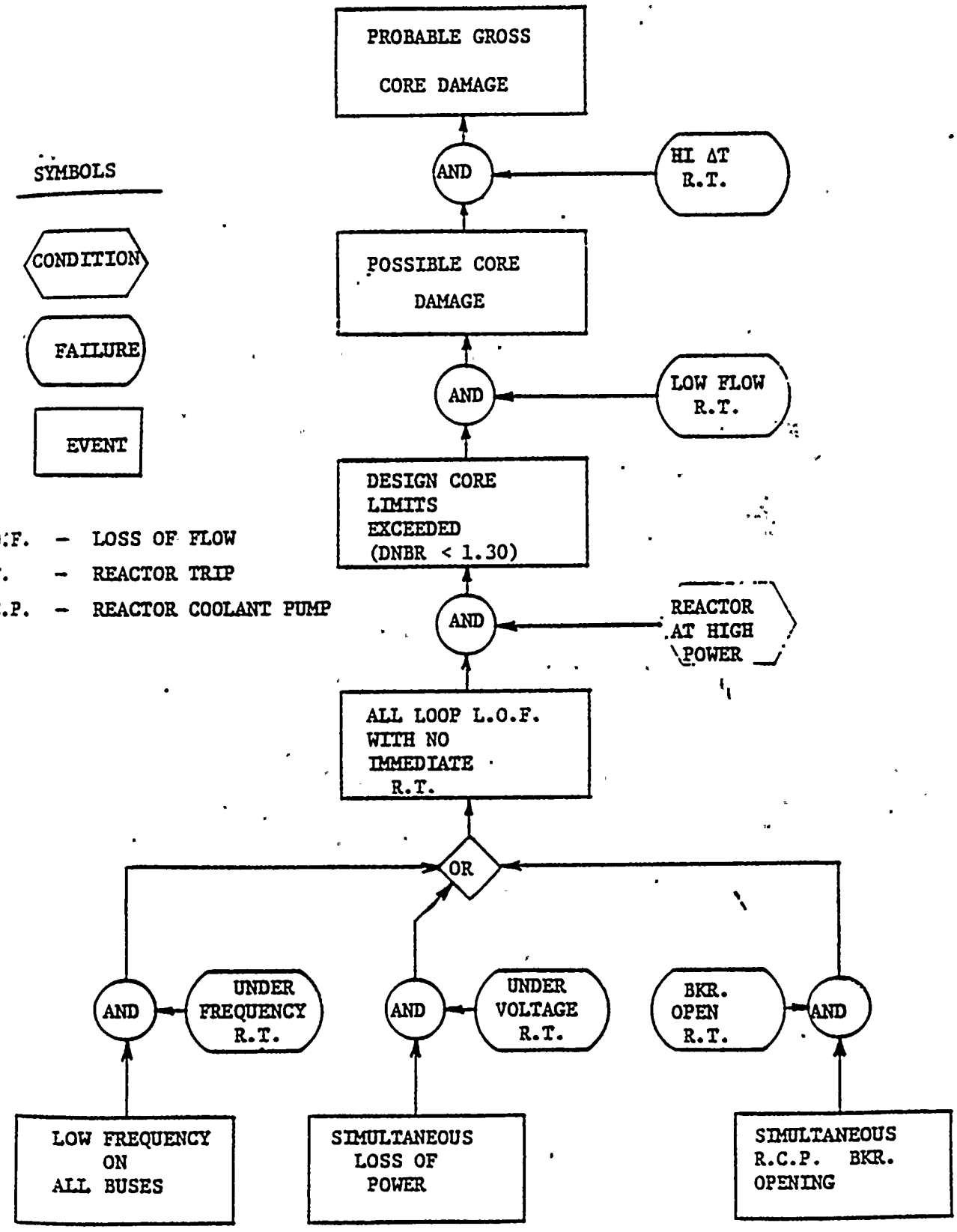


FIGURE 5.3-1

FAULT TREE FOR SINGLE LOOP LOSS OF FLOW

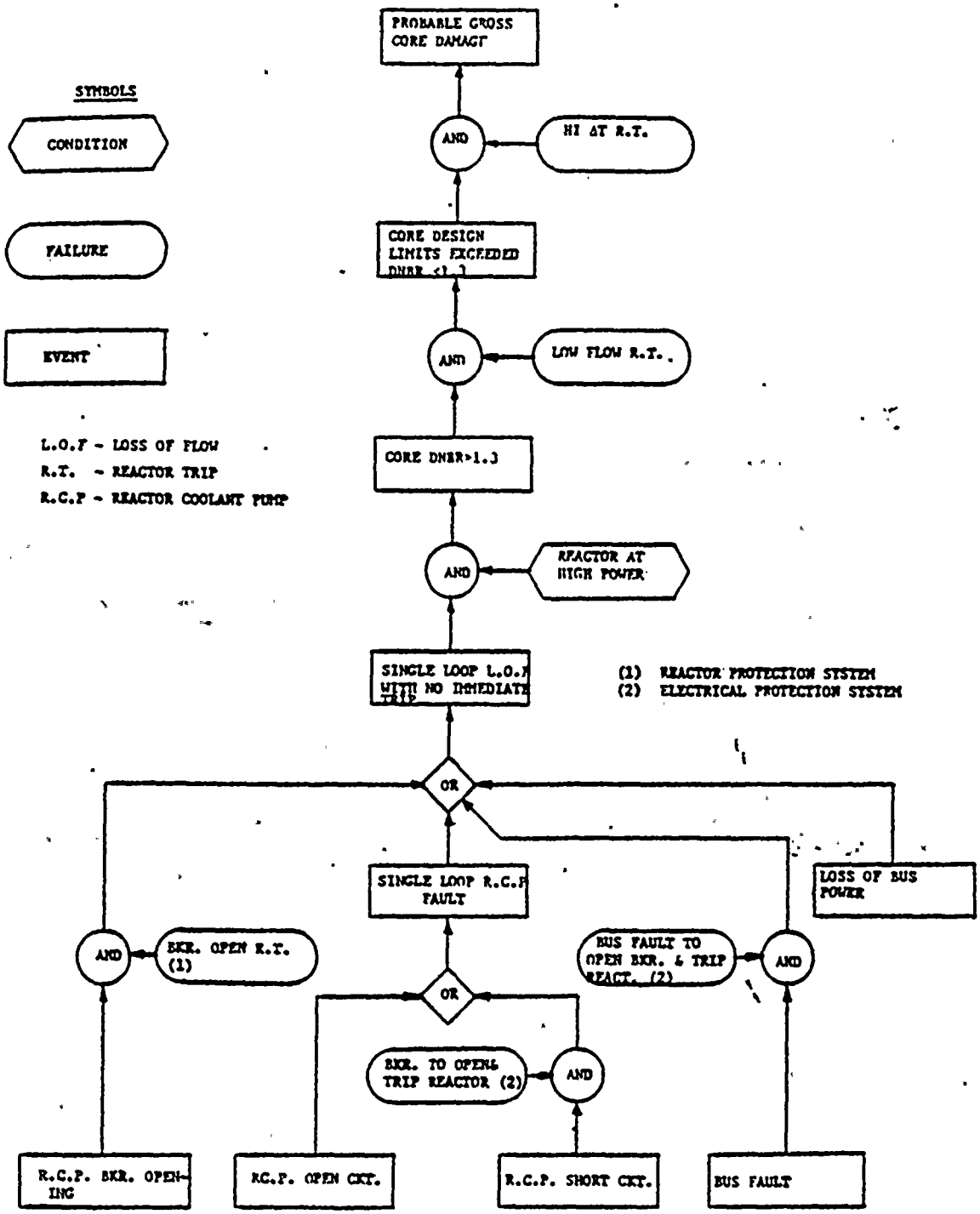
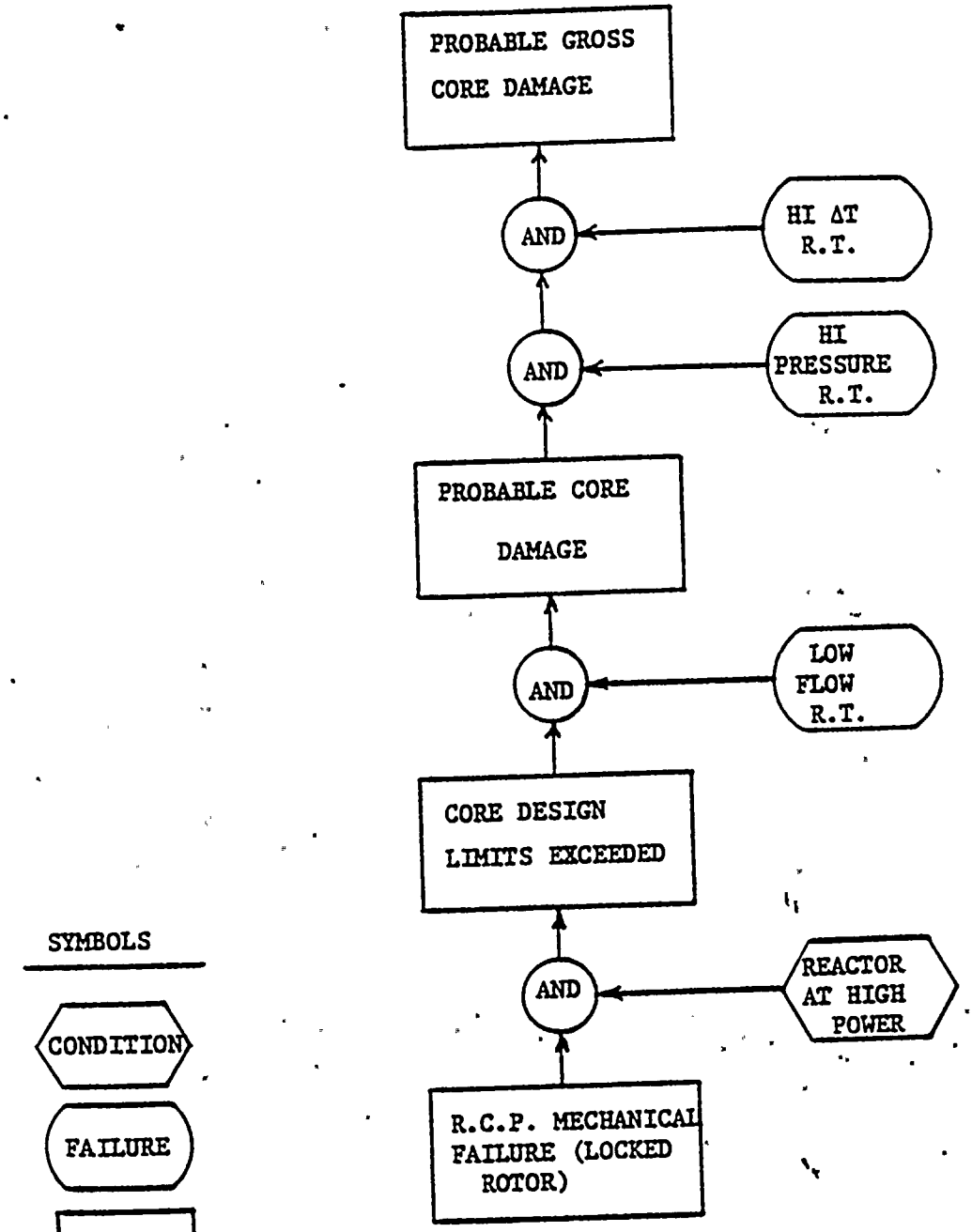


FIGURE 5.3-2

FAULT TREE FOR LOCKED ROTOR ACCIDENT



R.T. - REACTOR TRIP

R.C.P. - REACTOR COOLANT PUMP

FIGURE 5.3-3

MULTI-LOOP LOSS OF FLOW, TYPICAL PLANT

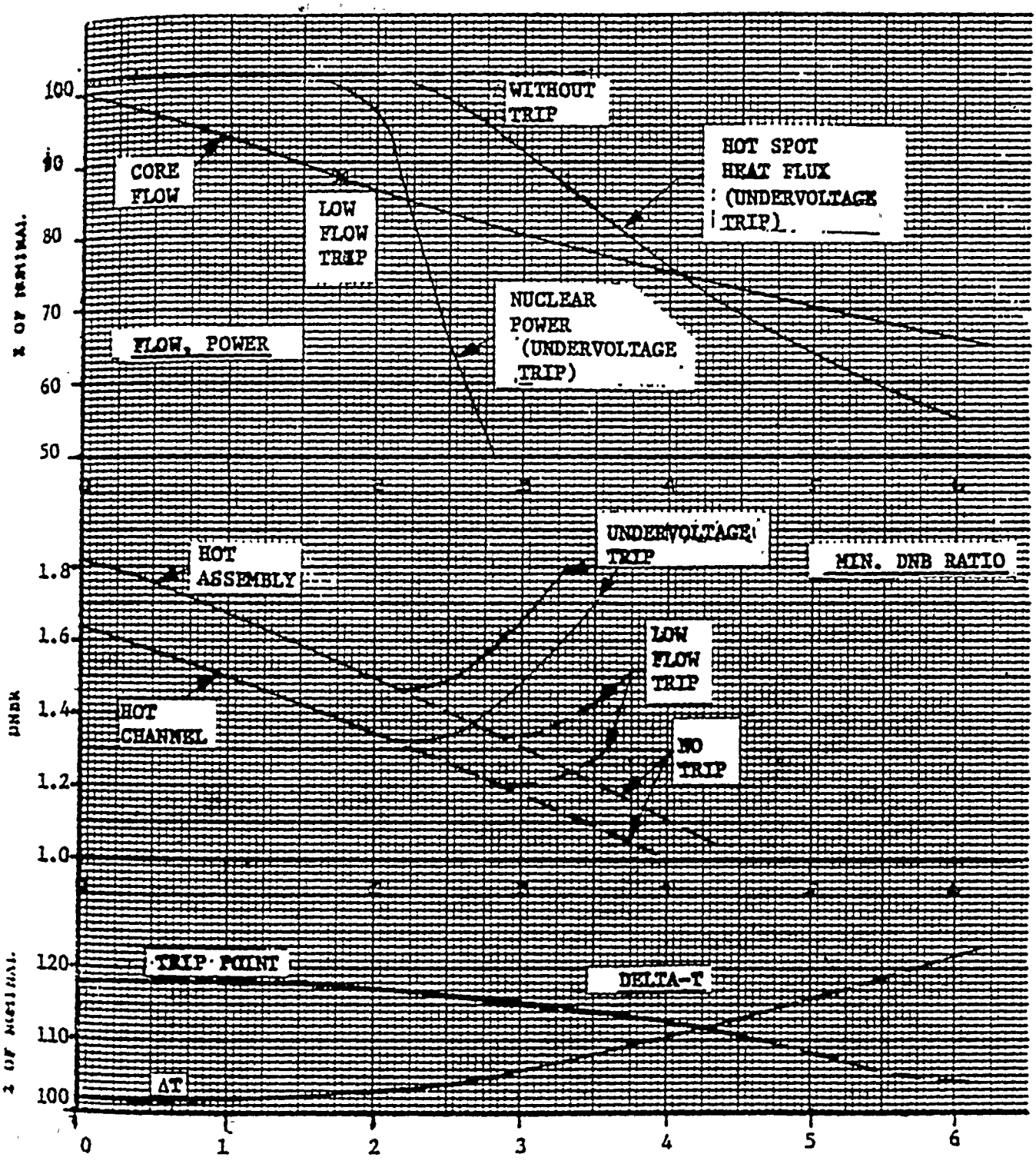
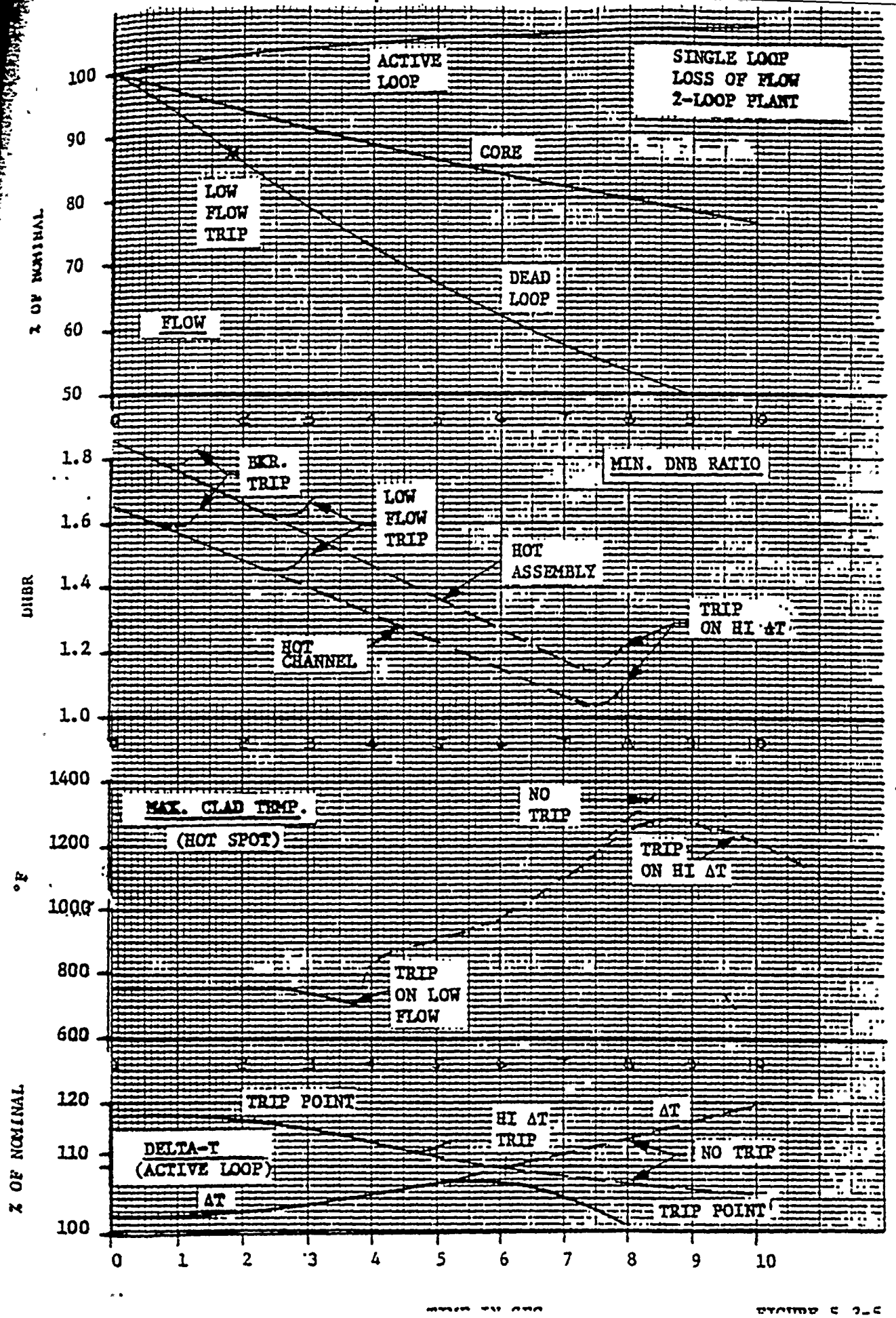
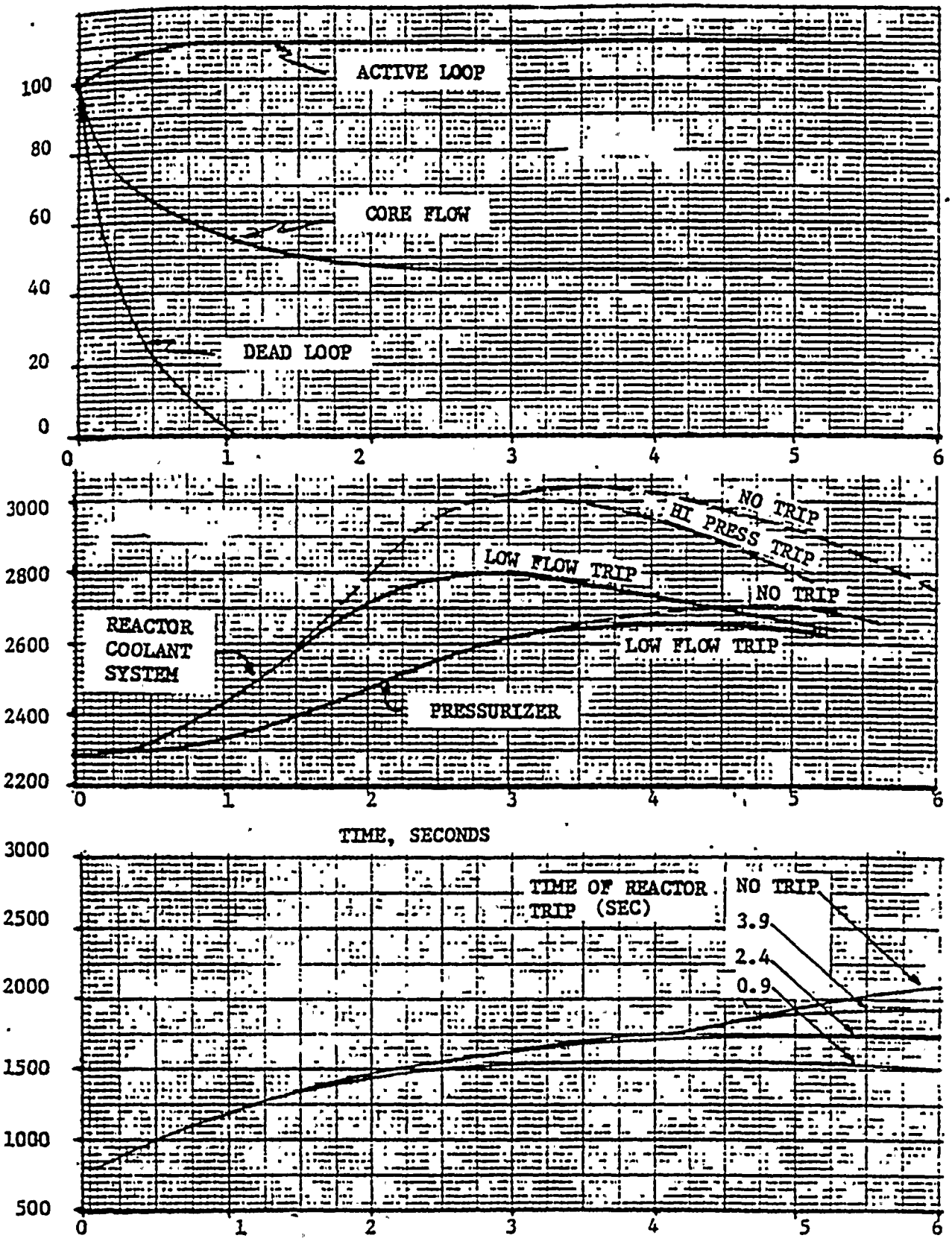


FIGURE 5.3-4


SINGLE LOOP
LOSS OF FLOW
2-LOOP PLANT
ACTIVE LOOP
CORE
LOW FLOW TRIP
DEAD LOOP
FLOW
% OF NOMINAL
100
90
80
70
60
50
MIN. DNB RATIO
BKR. TRIP
LOW FLOW TRIP
HOT ASSEMBLY
TRIP ON HI ΔT
HOT CHANNEL
DNBR
1.8
1.6
1.4
1.2
1.0
MAX. CLAD TEMP.
(HOT SPOT)
NO TRIP
TRIP ON HI ΔT
1400
1200
1000
800
600
°F
TRIP ON LOW FLOW
TRIP POINT
HI ΔT TRIP
ΔT
NO TRIP
DELTA-T (ACTIVE LOOP)
ΔT
TRIP POINT
% OF NOMINAL
120
110
100
0
1
2
3
4
5
6
7
8
9
10

LOCKED ROTOR, LOSS OF FLOW

2-LOOP PLANT



5.4 ROD EJECTION ANALYSIS

5.4.1 INTRODUCTION AND SUMMARY

The primary protection for a rod ejection accident is a reactor trip on high nuclear flux. The nuclear flux instrumentation is made up of four completely separate sensors and channels, and reactor trip is actuated if any two channels indicate high power. Analysis has been conducted to determine the consequences of a hypothetical failure of all the nuclear channels coupled with a hypothetical rod ejection accident.

Analysis, made on the basis of the Ginna Nuclear Plant of Rochester Gas & Electric Co. (RG&E), indicate that in the majority of rod ejection cases no protection is required (for example, ejection of a rod from its normally-expected position). It is further shown that the Delta-T trip provides an acceptable second level of defense for some cases. However, protection can not be demonstrated for some of the more severe full power cases. Protection may in fact exist, but it is not possible to positively demonstrate this with the currently available models.

An analysis of the available trip has been made, and is compared with an arbitrary clad limit of 2750°F and an arbitrary pressure limit of 3000 psi.

Two detailed cases are presented: a severe case from zero power end of core life, and a moderate case from full power end of core life. No reactor trip has been assumed for either case.

5.4.2 CASES CONSIDERED IN DETAIL

Zero Power Case

The case considered represents a rod ejection accident for an end of life core. The assumed ejected rod worth and hot channel factor are 1.0%δk and 12.5 respectively.

The resulting power transient and hot spot temperatures are detailed in Figure 5.4-1.

The final steady power level is conservatively assumed to be 15% of full power. This power level is lower than the value which one might normally expect for a rod reactivity insertion of 1.06k, owing to the high feedback weighting factors. (The large hot channel factors results in a large power change in the hot spot, where the statistical weight is high). The prompt burst results in a reactivity undershoot which, combined with the shortage of delayed neutrons, temporarily forces the power to a value below equilibrium condition. The power level is assumed to ramp up to 15% at 5 seconds after ejection, although calculations indicated that it would take much longer to reach this power level.

The plotted hot spot temperatures indicate that equilibrium conditions can be sustained. It is therefore concluded that no protection is required for this accident.

In general, the ejected rod worths and hot channel factors are lower for the beginning of life zero power cases, and therefore the consequences are expected to be somewhat less severe.

Full Power End of Life Case

The case presented is for a rod ejection accident occurring at the end of core life with an ejected rod worth of 0.33ôk and a hot channel factor of 3.23. The power transients and hot spot temperatures are detailed in Figure 5.4-2. The equilibrium power level is 112% of full power.

The peak cladding temperature of 2950°F occurs some 50 seconds after ejection. Under equilibrium conditions, some 50% by volume of the hot spot fuel is melted. A reactor trip on overpower Delta-T occurs at 6 seconds, limiting clad temperature to about 2400°. This case represents a severe accident, but is not intended to represent a limit.

A similar rod ejection accident, occurring at the beginning of life, would result in an equilibrium power level of about 125% of full power, with an equilibrium cladding temperature of the order 3100°F to 3200°F.

5.4.3 BACK-UP TRIP PROTECTION

The most limiting cases occur at or near full power. The Protection System is examined to determine under what circumstances a trip signal would terminate a rod ejection accident at full power. The results of the study are illustrated in Figure 5.4-3.

The graph is a plot of total excess nuclear energy addition versus time. Steady full power operation results in a locus covering the horizontal axis.

The nuclear flux trip is represented by a straight line of gradient 0.18, corresponding to a power level of 118%. Note that this line is an upper limit, and its position is in fact dependent on the power versus time shape. This is a general, but not important, effect for the lines plotted.

A rise in nuclear power produces a pressure surge. However, the effect is attenuated by the heat transfer time constant of the fuel (of the order of 4 seconds), and the possible relieving effect of the hole in the vessel head and relieving capacity of the power-operated relief valves. The high pressure trip could not be expected for any rod ejection accident.

The high Delta-T trip furnishes a backup trip for any severe rod ejection accident. Except in the most severe cases, it limits the clad temperature to less than 2750°F. Transport delays in the coolant loop delay the trip for several seconds.

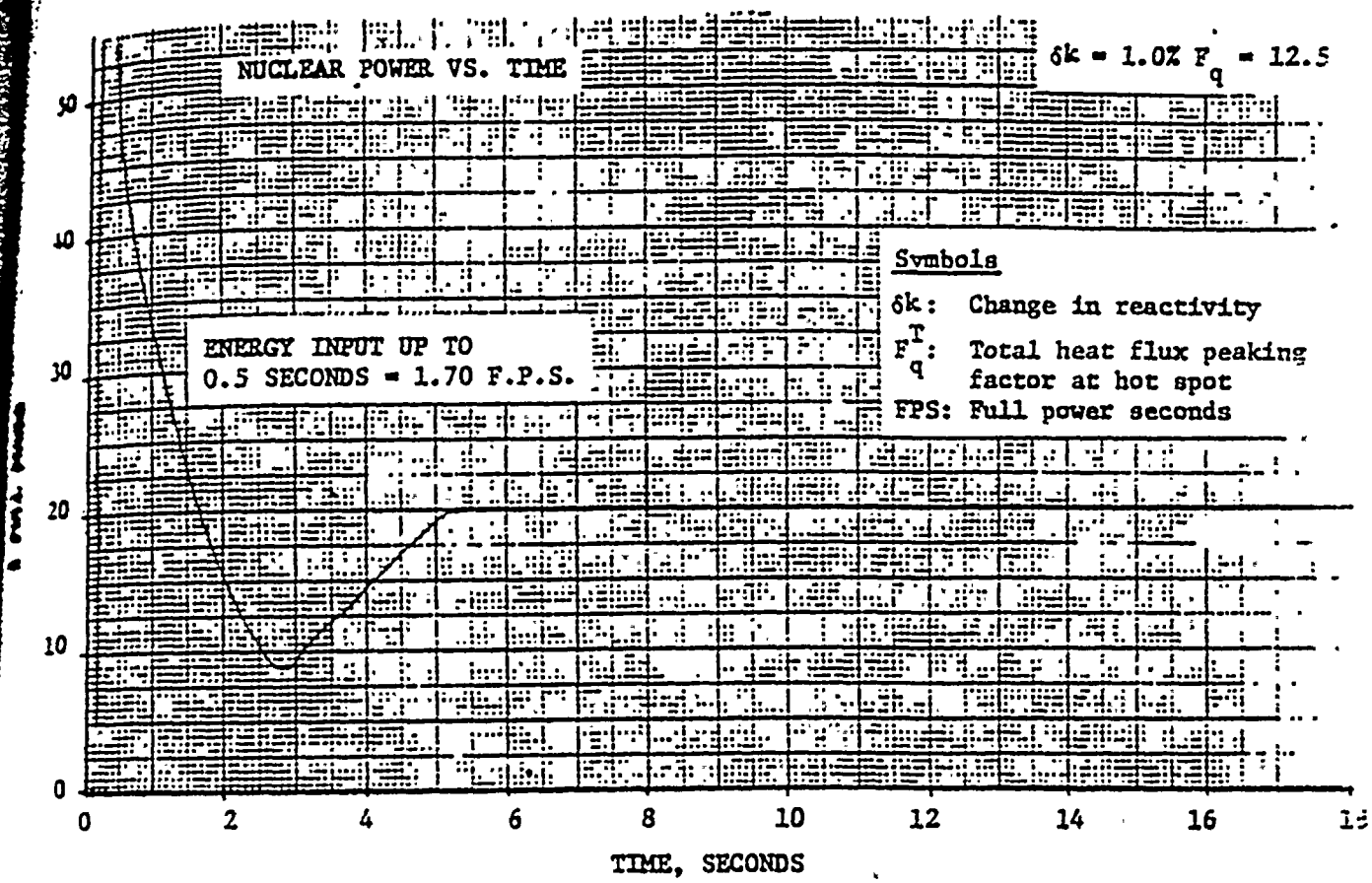
Also plotted on the graph are two arbitrary limit lines. They are respectively a clad limit of 2750°F* and a Coolant System pressure of 3000 psi. Both these limits have been arbitrarily selected and are not intended to represent physical limits. A power burst of some six full power seconds at time zero results in both these limits being reached some two to three seconds later. This is not a physically reliable condition for any Westinghouse reactor.

Figure 5.4-4 shows the power transients for rod ejection accidents occurring at end of core life for various ejected rod worths.

---

* These lines are based on steady-state and transient hot channel factors of 3.23.

ZERO POWER END OF LIFE ROD EJECTION, NO TRIP



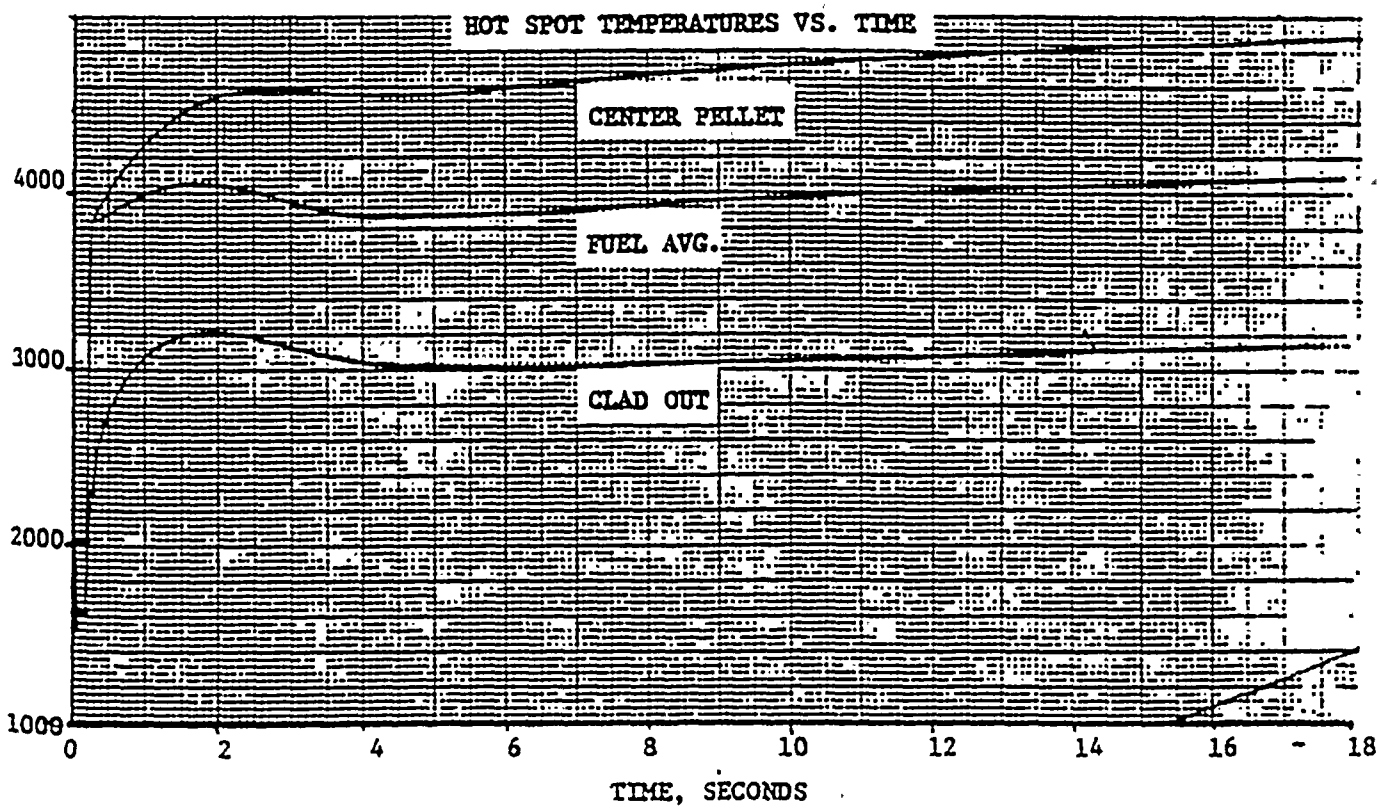
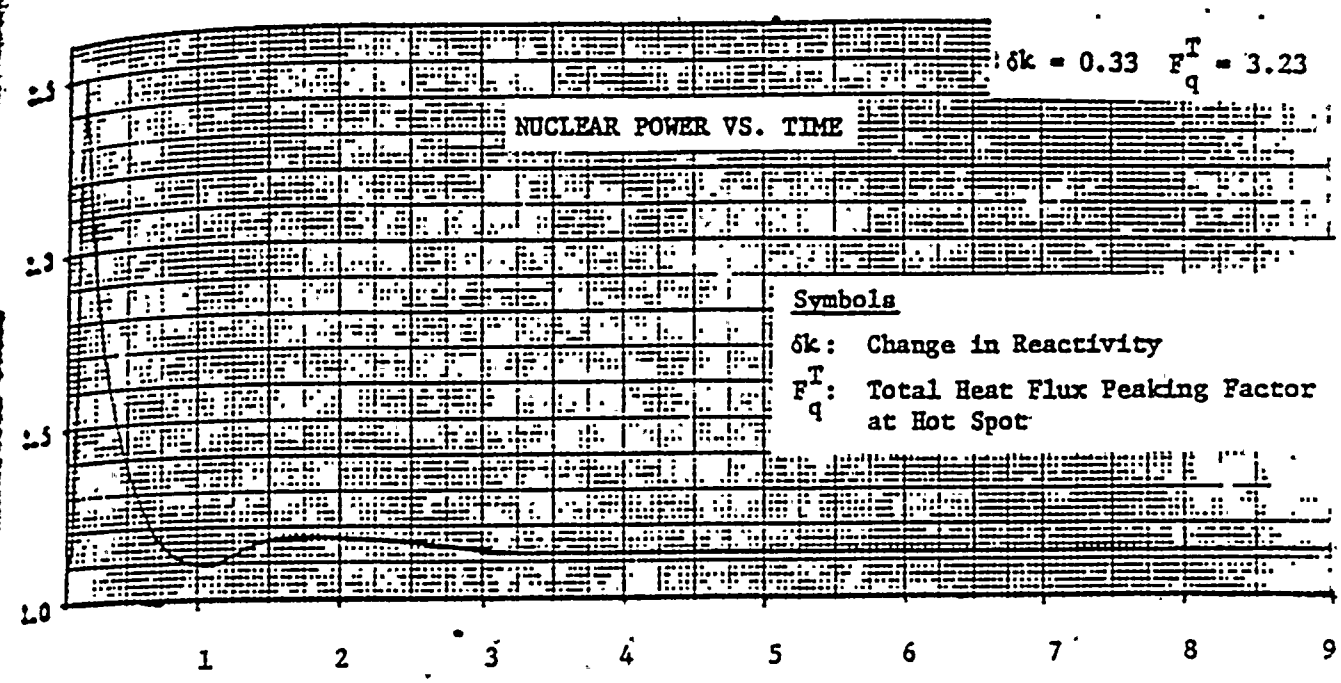


FIGURE 5.4-1

FULL POWER END OF LIFE ROD EJECTION, NO TRIP



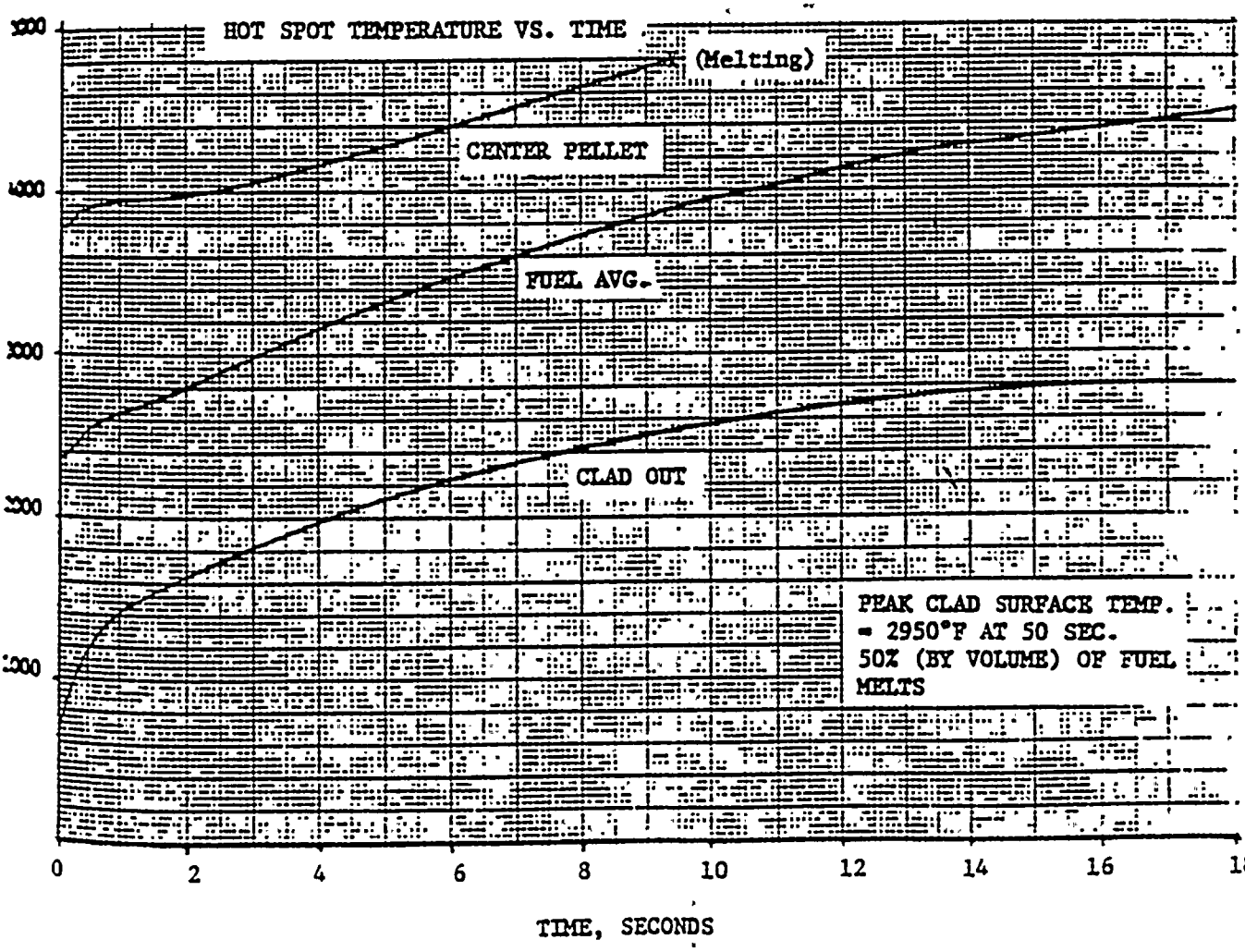


FIGURE 5.4-2

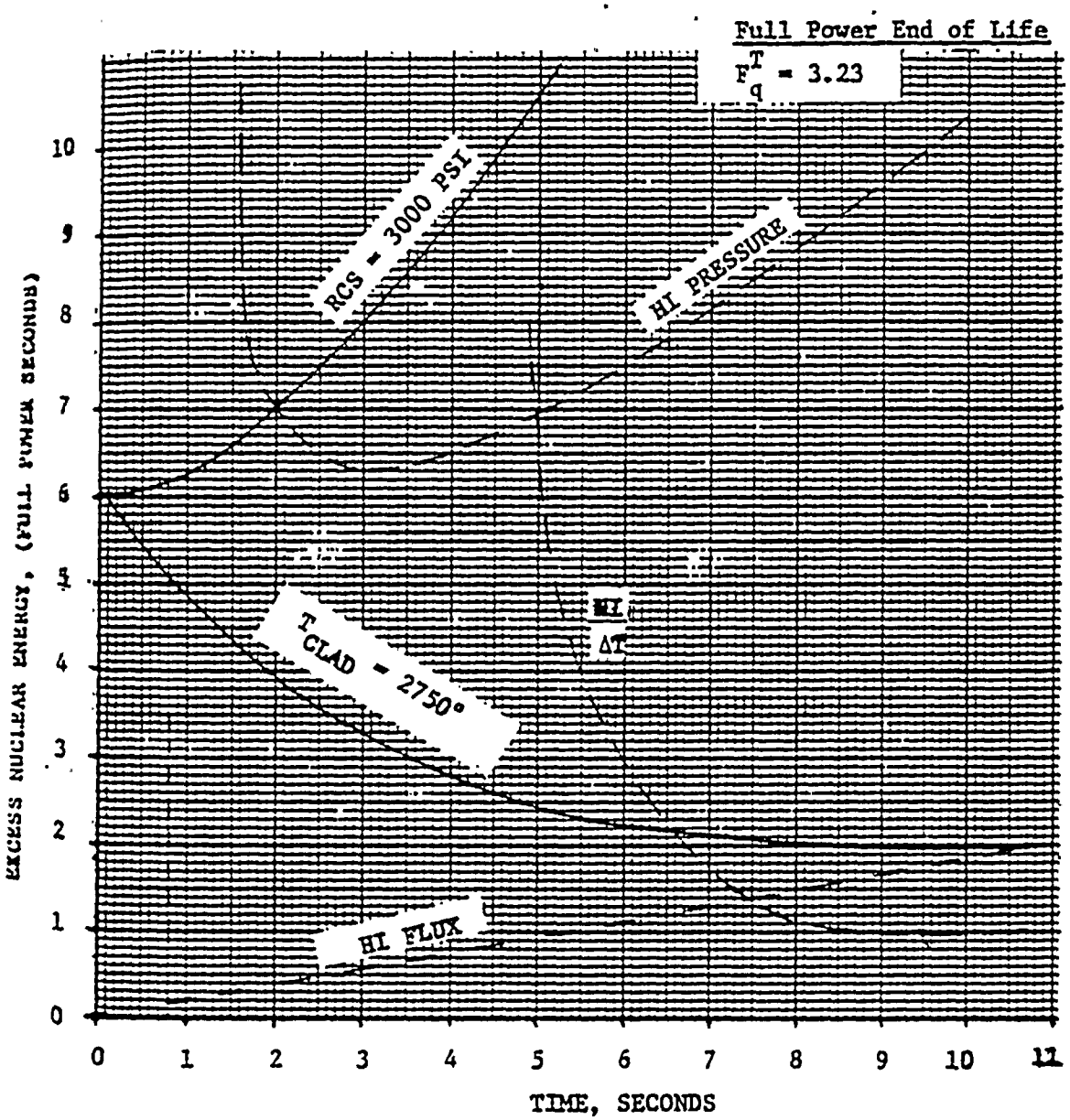


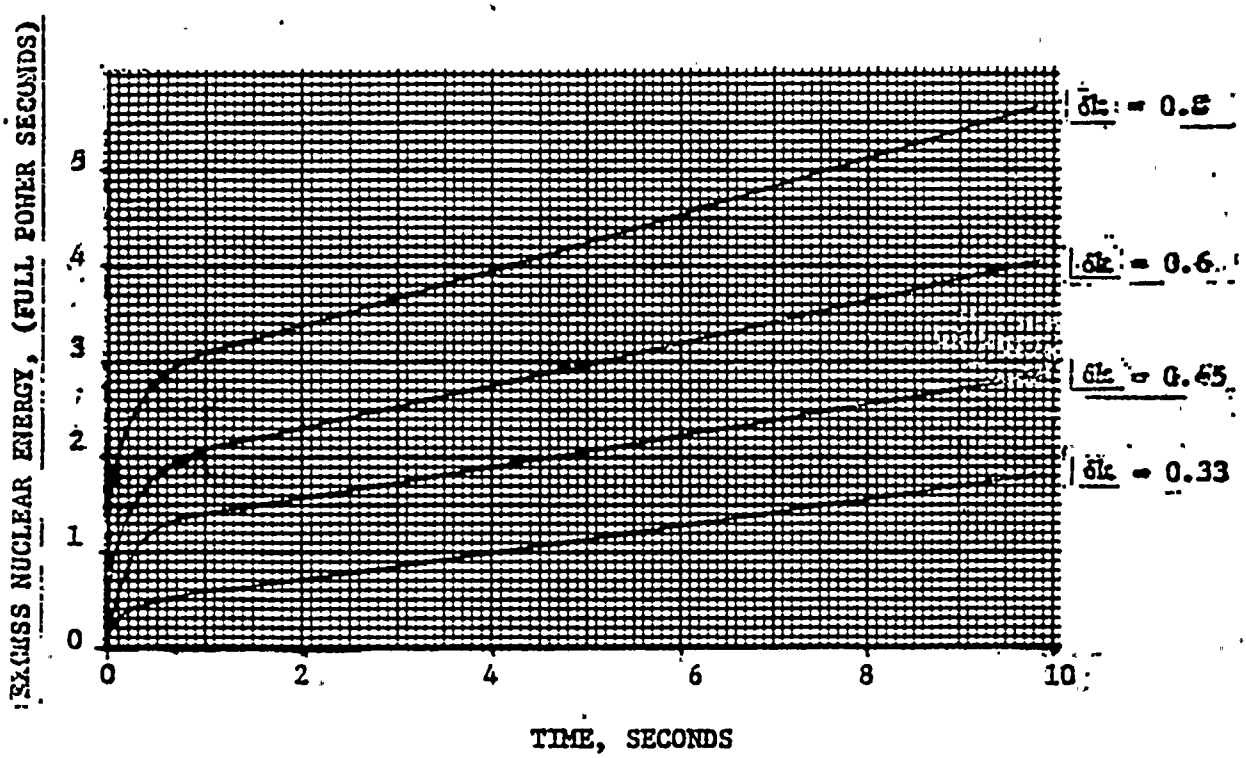
ILLUSTRATION OF SAFETY LIMITS AND TRIP POINTS FOR ROD EJECTION ACCIDENTS, NO TRIP

——— represents the locus of points at which trip would terminate the accident

——— represents locus of safety limits

FIGURE 5.4-3

FULL POWER END OF LIFE ROD EJECTION WITHOUT TRIP



Note: 0.4% $\overline{\delta k}$ represents a practical limit for full power cases.

ILLUSTRATION OF TRANSIENT TRAJECTORIES FOR ROD EJECTION ACCIDENTS WITH NO TRIP

FIGURE 5.4-4

5.5 LOSS OF STEAM LOAD

5.5.1 INTRODUCTION AND SUMMARY

A loss of steam load may be caused by closing of the turbine stop valves, which normally follows a turbine trip signal; by closing of the turbine control valves following a rejection of electrical load; or by steam isolation following a Reactor Protection System signal. The consequences of a loss of steam load are a rapidly increasing Steam System pressure and Reactor Coolant System temperature and pressure due to the loss of heat sink.

Protection instrumentation is provided to immediately trip the reactor following a turbine trip signal. A steam line isolation signal is normally accompanied by a safety injection signal and also results in a reactor trip. Following a rejection of electrical load, a Steam Dump System acts to prevent reactor trip by automatic steam dump to the condenser. (Up to 100% load rejection can be handled by some plants.) If the load rejection greatly exceeds the steam dump capacity, or if the Steam Dump System should fail to operate, a reactor trip may occur on high pressure. Redundant protective instrumentation and conservative design of pressure relief devices assures the safety of the plant for a large load rejection without recourse to Automatic Rod Control, Pressurizer Pressure Control, or Steam Dump Control Systems.

In this report, the Protection System is examined to see if diverse protection exists for a complete loss of load without direct reactor trip. Diversity is found to exist to protect the Reactor Coolant System and reactor core.

5.5.2 LOSS OF LOAD PROTECTION AND DESIGN CRITERIA

The reactor is protected for loss of load by:

a) Steam dump to condenser (actuated by the Control System)

b) Pressurizer pressure relief (safety valves and power-operated relief valves)

c) Steam System pressure relief (safety valves and power-operated relief valves)

d) Direct reactor trip (on turbine trip)

e) High pressurizer pressure trip

f) Overtemperature ΔT trip

g) High pressurizer level trip.

Steam Dump to Condenser

The Steam Dump System acts automatically upon sensing a loss of load greater than a preset amount. The steam dump valves are then either modulated or tripped open until the Reactor Coolant System temperature reaches the new programmed load reference temperature. The reactor power is reduced by control rod insertion during this time. In case of a turbine trip or reactor trip, the steam dump is actuated and controlled on a preset no-load reference temperature.

The Steam Dump Control System is described in Section 3.2.

Pressurizer Pressure Relief

The pressurizer safety valves are sized to match the maximum volumetric surge rate associated with a complete loss of load without steam dump or a direct reactor trip. This is not dependent on pressurizer pressure control. The pressurizer safety valves therefore completely protect the Reactor Coolant System against overpressure, independent of the high pressure reactor trip.

The relief valves are sized to prevent actuation of the high pressure trip when the steam dump and rod drive systems work, and the required steam relief is within the capacity of the Steam Dump System.

Steam System Pressure Relief

The Steam System safety valves pass 100% of maximum calculated turbine steam flow, at the safety valve set pressure plus accumulation. This allows the plant to accept a 100% load rejection without reactor trip or steam dump without overpressurizing the Steam System.. In addition, relief valves set to open at a lower pressure are also provided, and are typically sized at about 10% of the safety valve capacity.

Direct Reactor Trip

The most common cause of a loss of load is a turbine-generator trip. In the event of such a trip, the turbine stop valves close. A turbine

trip sensed by 2/3 low auto-stop oil pressure or 2/2 stop valve closure results in a reactor trip if the reactor is at high power. The purpose of these trips is to minimize the thermal transient and steam dump requirements for these relatively frequent plant transients.

High Pressurizer Pressure Trip

There is a reactor trip on 2/3 high pressurizer pressure, generally set to 2400 psia, or slightly above the pressurizer power operated relief valve setting and below the pressurizer safety valve opening pressure.

Overtemperature ΔT

The purpose of this trip is to protect the core against any combination of reactor coolant temperature, power or pressure which could cause DNB. Trip logic is 2/4 for 2 and 4-loop plants and 2/3 for 3-loop plants.

High Pressurizer Level Trip

This trip acts to prevent water discharge from the pressurizer safety valves. Logic is 2/3.

5.5.3 EVALUATION OF PROTECTION SYSTEM FOR LOSS OF LOAD

A complete loss of load without steam dump and without a direct reactor trip is evaluated to find if diverse protection exists to prevent a hazard to the integrity of the plant through overpressurization or DNB. The transient was investigated for a current, high power density plant, and no credit was taken for power reduction due to automatic control rod motion or moderator temperature coefficient.

Initiation of Accident

Figure 5.5.1 shows a fault tree for a loss of load without steam dump, with the reactor at high power and no direct reactor trip. One way a loss of load can occur is by closing of the turbine stop valves following a turbine trip signal or by hydraulic fluid pressure failure (the valves are held open by hydraulic fluid). However, one and possibly two trips must then fail in order to prevent an immediate reactor trip.

Another possible failure mode is a turbine runback caused by the throttle valves closing. This could be initiated by a rod drop, an overpower or overtemperature ΔT signal, by an actual or spurious loss of electrical load signal, or by a failure in the turbine controller and load limit system. A spurious rod drop signal would normally decrease the turbine load by a fixed small percentage of full load. The control

valve could close completely only if an improper circuit exists in the controller. Similarly, an overpower or overtemperature ΔT signal normally causes a step load decrease of 5% every 30 seconds; and only in the case of a simultaneous failure or improper circuit in the controller could there be insufficient time for the operator to take notice. If the turbine runback is caused by an overpower or overtemperature ΔT Protection System failure, the failure could only be in the safe direction; that is, the error or failure would be in the direction to cause a reactor trip.

A third possible path for a loss of load is through steam line isolation. This may occur either through a loss of air supply to the isolation valves, or by a spurious or real isolation signal from the Reactor Protection System.

As a result of the loss of steam flow to the turbine by any of the three paths outlined above, the Steam Dump System is activated. However, no credit can be taken for this following steam line isolation, since the dump valves are downstream of the isolation valves. For all three paths, the resulting decrease in first stage turbine impulse pressure causes automatic reactor power reduction by control rod insertion. Even if the reactor is in manual control, the moderator coefficient of reactivity is generally negative and would cause a power decrease as temperatures increase.

The fault tree shown on Figure 5.5.1 indicates that, in most cases, a fault could cause a complete loss of load with no steam dump or reactor power decrease only if one or more simultaneous failures of the Control or Protection System also resulted. However, the following analysis is based on a complete loss of steam load without steam dump, reactor control, or direct reactor trip.

Analysis and Discussion

Figure 5.5.3 shows the results of a transient analysis for a complete loss of load without steam dump. The results show that the safety valves capacity of the Steam System is sufficient to limit the pressure rise to less than 1150 psia, even without a reactor trip. The Reactor Coolant System T_{avg} transient is shown for a high pressurizer pressure or high pressurizer level reactor trip, as well as for no trip.

Actuation of the Steam System safety valves restores the reactor heat sink and causes a decrease in the rate of rise of the reactor coolant average temperature. Without a reactor trip, T_{avg} would eventually come into equilibrium when the required heat dissipation at the safety valve set pressure is reached.

The Reactor Coolant System pressure transient is also depicted in Figure 5.5.3. The effect of the pressurizer power operated relief valves is felt slightly above their set pressure of 2350 psia. Since the required

relief for a full loss of load without steam dump far exceeds the relief valve capacity, the pressure continues to rise to the safety valve set pressure of 2500 psia. The opening of the pressurizer safety valves, and the restoration of the secondary sink by steam relief, limits the Reactor Coolant System pressure rise. The surge rate decreases as the rate of rise of T_{avg} decreases, and eventually the pressure decreases to the relief valve opening pressure. The transient is also shown for the high pressurizer pressure and level reactor trips. The power operated relief valves delay the reaching of the high pressure reactor trip setpoint by about 2 seconds.

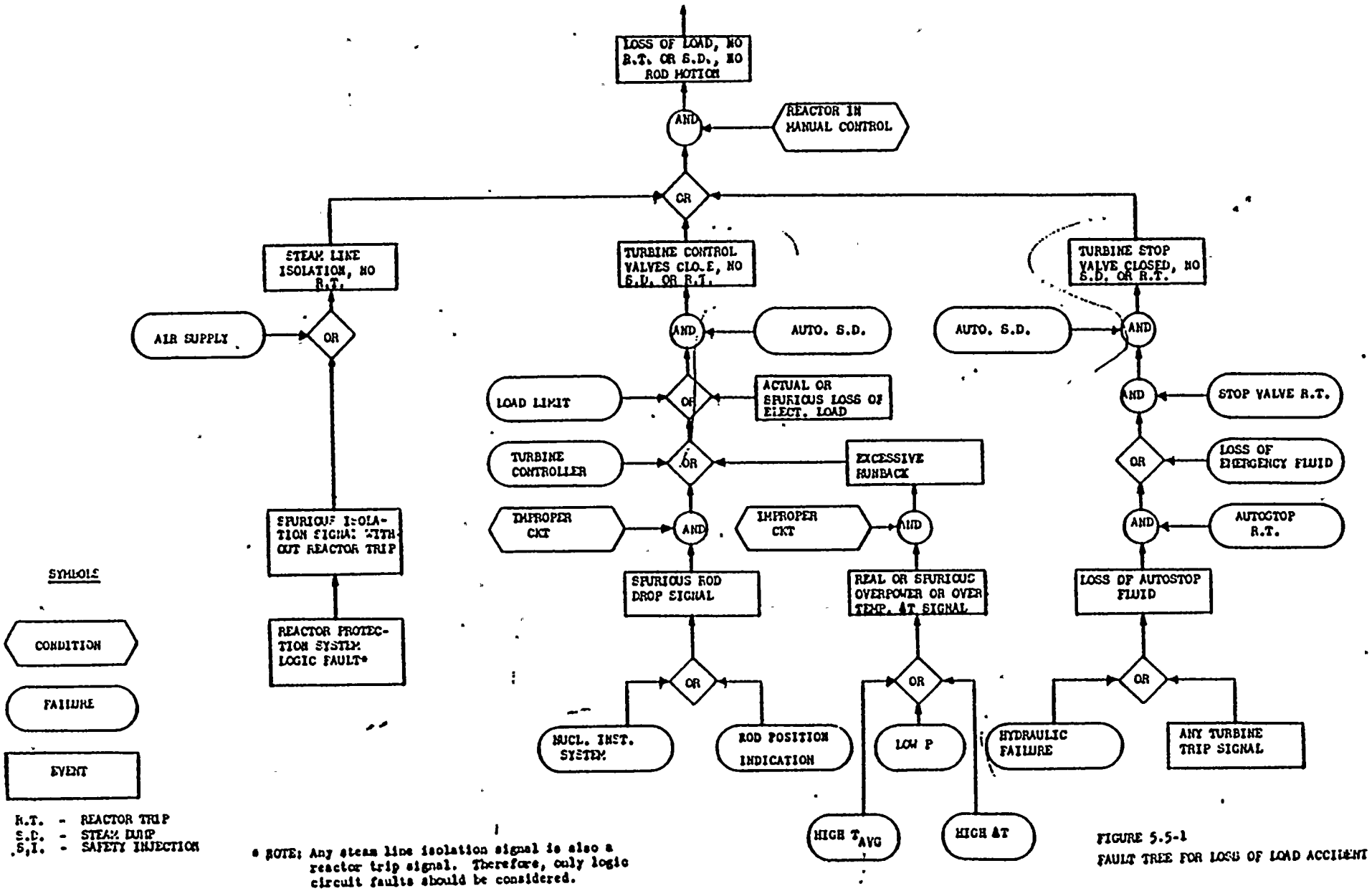
The lower graph in Figure 5.5.3 shows the minimum (hot channel) DNB transient. For the first few seconds, the DNB ratio rises due to the increasing system pressure, while piping delays cause the core inlet temperature to remain constant. Two trips, the high pressure and overtemperature ΔT reactor trips, prevent the core design limits from being exceeded. Rate compensation on T_{avg}, which is included in the overtemperature ΔT trip, would actually cause the trip setpoint to be reached much sooner than is depicted in the figure. The high pressurizer water level reactor trip is inadequate to prevent the core from exceeding the design limits. However, the minimum DNB ratio in the hot assembly for a high level trip is above 1.0 and would assure that core damage, if it occured at all, would be limited to a small fraction of the core. A conservative setpoint was assumed for the high level trip.

A fault tree for the accident, leading to core damage, is shown in Figure 5.5.2.

5.5.4 CONCLUSIONS

This accident is not considered likely since in most of the incidents which could cause it, one or more simultaneous failures of control or protection instrumentation must also occur. In addition, at any time other than early in core life, the large negative moderator coefficient would cause the accident to be self limiting and give much better results than depicted in this analysis. However, if the accident were to occur, diversity does exist in that three different levels of protection are available.

FIGURE 5.5-2



* NOTE: Any steam line isolation signal is also a reactor trip signal. Therefore, only logic circuit faults should be considered.

FIGURE 5.5-1
FAULT TREE FOR LOSS OF LOAD ACCIDENT

FAULT TREE FOR CORE DAMAGE

LOSS OF STEAM LOAD

SYMBOLS

CONDITION

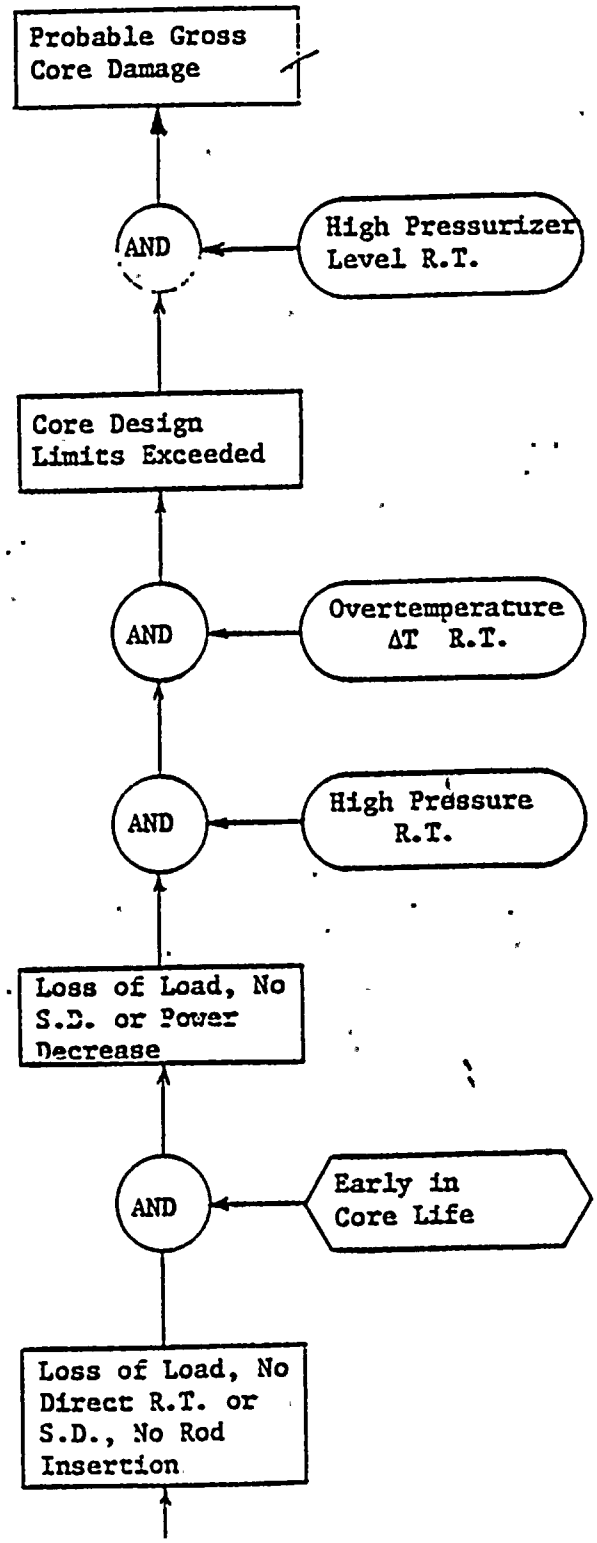
FAILURE

EVENT

R.T. - REACTOR TRIP

S.D. - STEAM DUMP

S.I. - SAFETY INJECTION



(See Figure 5.5-1)

FIGURE 5.5-2

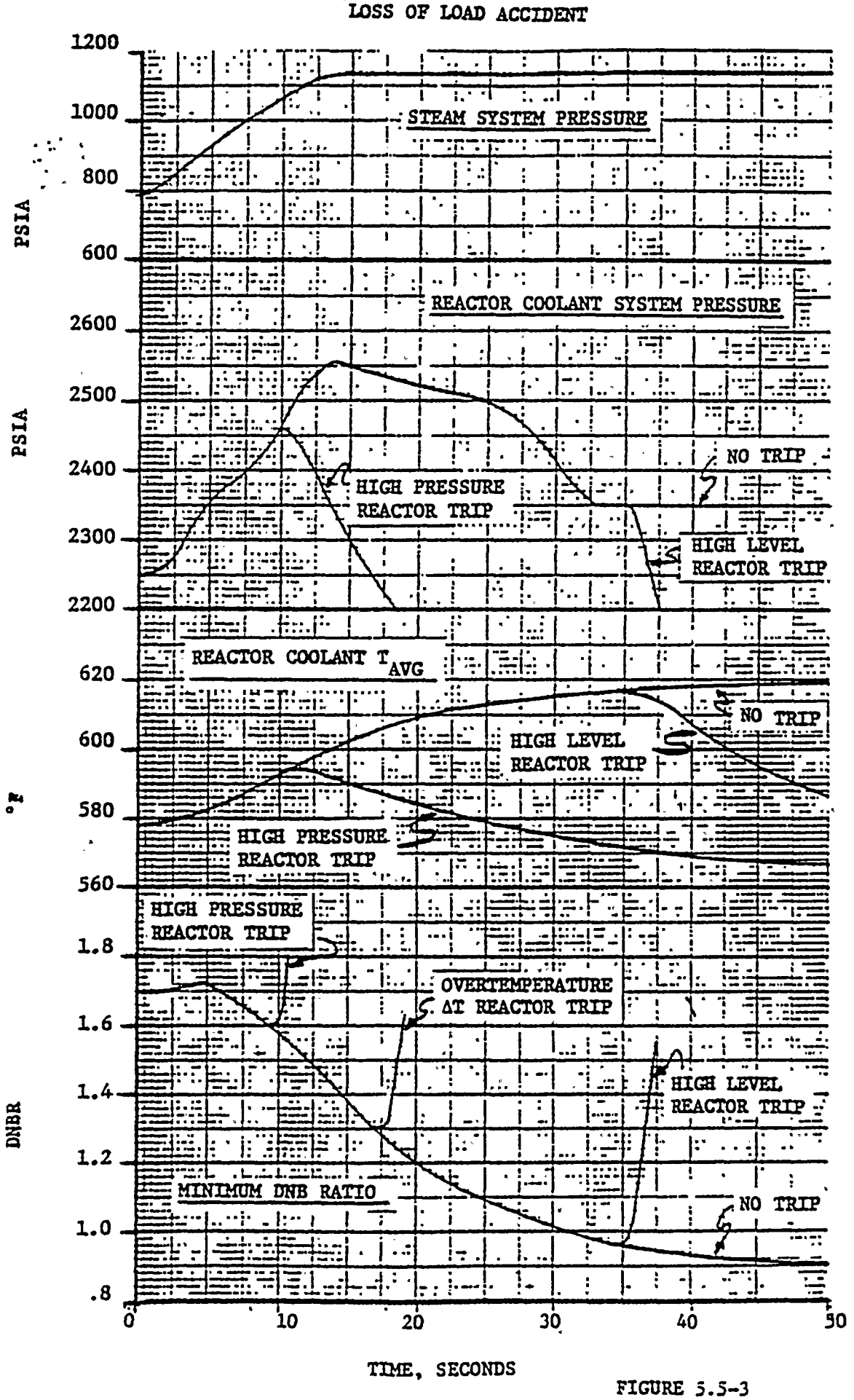

LOSS OF LOAD ACCIDENT
1200
1000
800
600
PSIA
STEAM SYSTEM PRESSURE
REACTOR COOLANT SYSTEM PRESSURE
2600
2500
2400
2300
2200
PSIA
NO TRIP
HIGH PRESSURE
REACTOR TRIP
HIGH LEVEL
REACTOR TRIP
620
600
580
560
°F
REACTOR COOLANT T_{AVG}
NO TRIP
HIGH LEVEL
REACTOR TRIP
HIGH PRESSURE
REACTOR TRIP
HIGH PRESSURE
REACTOR TRIP
1.8
1.6
1.4
1.2
1.0
.8
DNBR
OVERTEMPERATURE
ΔT REACTOR TRIP
HIGH LEVEL
REACTOR TRIP
MINIMUM DNB RATIO
NO TRIP
0
10
20
30
40
50
TIME, SECONDS

FIGURE 5.5-3

5.6 ROD WITHDRAWAL DURING STARTUP

Normal startup procedure is by control rod withdrawal under manual control. Malfunction of the rod control system or operator error can cause a reactivity excursion with a resultant rapid increase in power.

Rod withdrawal accidents in the power range are evaluated in Section 5.1. For these accidents, the power increase is approximately linear for a linear increase in reactivity. For accidents starting from very low power (startup range), the neutron flux may increase by many decades before there is significant Doppler feedback.

The nuclear power response to a continuous reactivity insertion from the startup range is characterized by a very fast rise terminated by the reactivity feedback effect of the negative fuel temperature coefficient (Doppler effect). This self-limiting effect is of prime importance during a startup accident since it limits the power to a tolerable level prior to external protective action. After the initial power burst, the nuclear power is momentarily reduced and then if the accident is not terminated, the nuclear power increases again but at a much slower rate.

Protection against startup accidents is provided by diverse types of neutron-monitoring instrumentation: source range, intermediate range, and power range channels. Major differences in the ion chamber and circuit design exist between the intermediate and power range channels. The source range uses a neutron sensor of a different principle: proportional counter rather than ionization chamber.

Should continuous control rod withdrawal be initiated and assuming the source and intermediate range alarms and indications are ignored, the transient will be terminated by any of the following automatic protective actions.

a) Source range flux level trip - actuated when either of two independent source range channels indicates a flux level above a preselected, manually adjustable value. This trip function may be manually bypassed when either intermediate range flux channel indicates a flux level above the source range cutoff power level. It is automatically reinstated when both intermediate range channels indicate a flux level below the source range cutoff power level.

b) Intermediate range rod stop - actuated when either of two independent intermediate range channels indicates a flux level above a preselected, manually adjustable value. This rod stop may be manually bypassed when two out of the four power range channels indicate a power level above approximately ten per cent power. It is automatically reinstated when three of the four power range channels are below this value.

c) Intermediate range flux level trip - actuated when either of two independent intermediate range channels indicates a flux level above a preselected, manually adjustable value. This trip function is manually bypassed when two of the four power range channels are reading above approximately ten per cent power and is automatically reinstated when three of the four channels indicate a power level below this value.

d) Power range flux level trip (low setting) - actuated when two out of the four power range channels indicate a power level above approximately 25 per cent. This trip function may be manually bypassed when two of the

four power range channels indicate a power level above approximately ten per cent power and is automatically reinstated when three of the four channels indicate a power level below this value.

e) Power range flux level trip (high setting) - actuated when two out of the four power range channels indicate a power level above a preset setpoint. This trip function is always active.

Since all protective actions in the above list are based on level set points, rather than rate set points, protection is not dependent upon having a rapid rate of power increase.

The standard startup accident analysis reported in Safety Analysis Reports takes credit for only the power range protection. However, the intermediate range high flux reactor trip is always in service below 10% power, and would also serve to terminate the accident. Further, any accident starting from a subcritical condition would be terminated by the high source range reactor trip. Therefore, Protection System deversity exists for startup accidents.

Figures 5.6-1 and 5.6-2 show the calculated transient response of nuclear flux and fuel temperatures for a startup accident with a high rate of reactivity insertion.

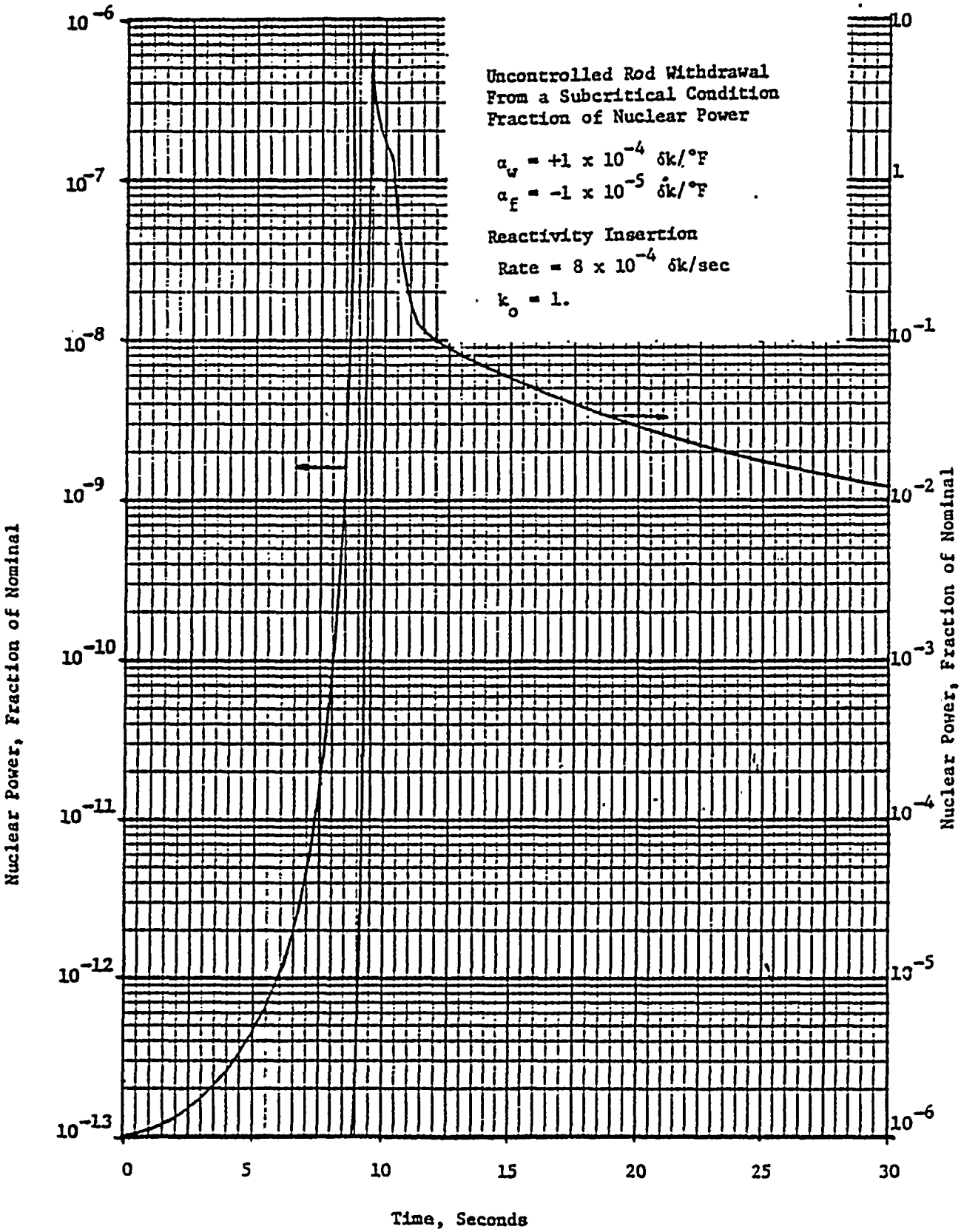

Uncontrolled Rod Withdrawal
From a Subcritical Condition
Fraction of Nuclear Power
α_w = +1 x 10^{-4} δk/°F
α_f = -1 x 10^{-5} δk/°F
Reactivity Insertion
Rate = 8 x 10^{-4} δk/sec
k_o = 1.
Nuclear Power, Fraction of Nominal
10^{-6}
10^{-7}
10^{-8}
10^{-9}
10^{-10}
10^{-11}
10^{-12}
10^{-13}
10
1
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
Nuclear Power, Fraction of Nominal
0
5
10
15
20
25
30
Time, Seconds

FIGURE 5.6-1

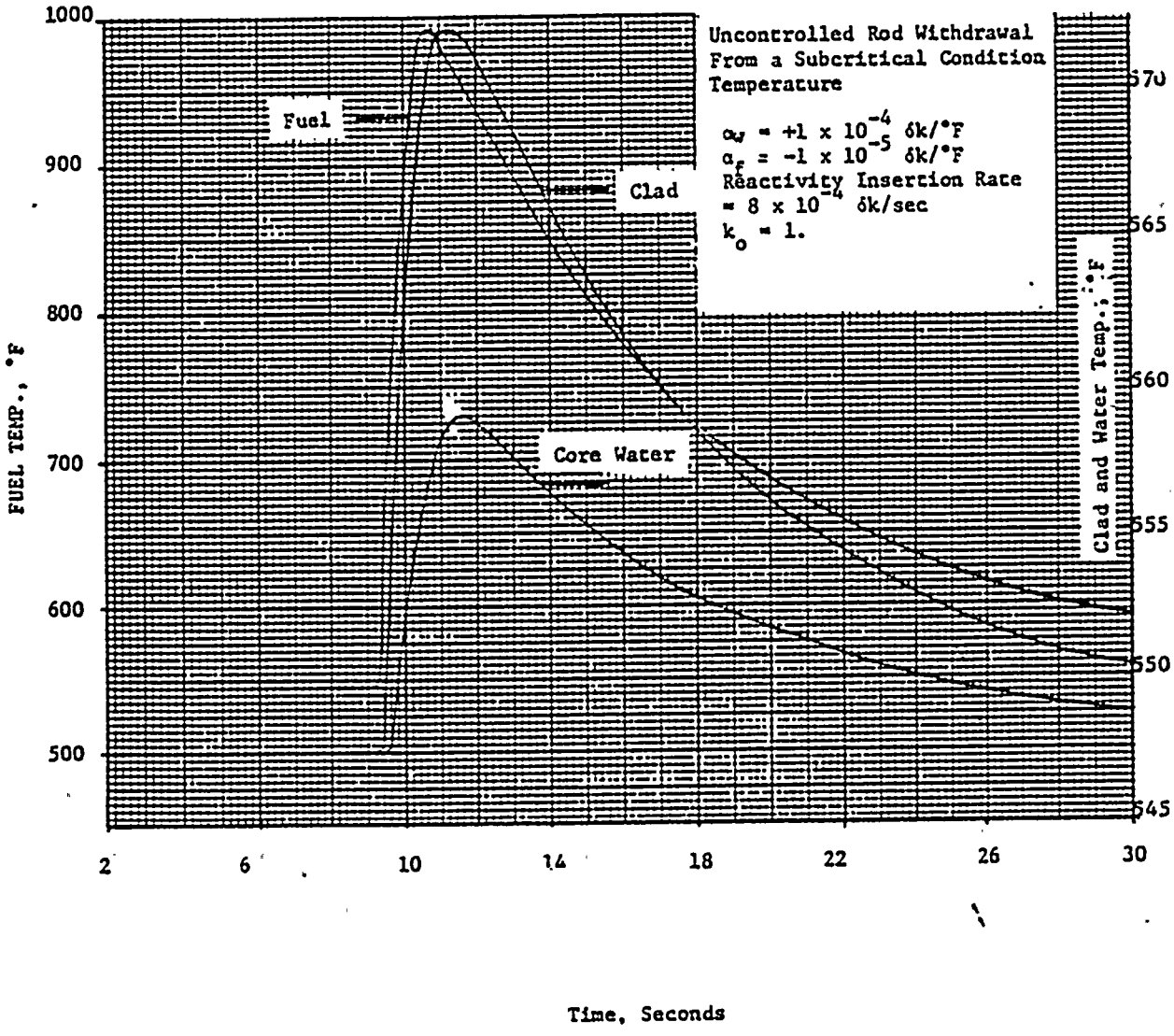

Uncontrolled Rod Withdrawal
From a Subcritical Condition
Temperature
$\alpha_w = +1 \times 10^{-4}$ δk/°F
$\alpha_f = -1 \times 10^{-5}$ δk/°F
Reactivity Insertion Rate
$= 8 \times 10^{-4}$ δk/sec
$k_o = 1.$
Fuel
Clad
Core Water
FUEL TEMP., °F
Clad and Water Temp., °F
1000
900
800
700
600
500
570
565
560
555
550
545
2
6
10
14
18
22
26
30
Time, Seconds

FIGURE 5.6-2

5.7 CONTROL ROD DROP

De-energizing a drive mechanism causes a full-length control rod to fall into the core. (Part-length rods fail "as-is" when de-energized.) This causes an immediate decrease in core power, most noticeable in the region of the dropped rod. If the average core power is returned to its original valve, most of the core would be at a higher power density because of the local depression in the region of the dropped rod.

During the initial design for the current generation of Westinghouse PWR's, the increase in hot channel factors for a dropped rod was not known. It was therefore assumed that DNB might result if the core were allowed to return to full power following a rod drop. Protective circuits were designed accordingly and classified as part of the Protection System. The design requirement for this protective function was to insure that, following a dynamic rod drop, the reactor would not return to a power level high enough to cause a DNB ratio less than 1.30. Mechanisms which would tend to restore initial core power are normal automatic control and plant cooldown with a negative moderator coefficient.

However, recent physics analysis for malpositioned control rods has shown that, in every case for an inserted rod, full power operation would not cause a DNB ratio less than 1.30. Because the local power decrease causes a general power increase throughout the rest of the core, the increase in hot channel factors is limited to approximately 15% or less, depending on core size. With respect to DNB, this is equivalent to 15% overpower. Core DNB design

margins of this magnitude must exist at full power to allow for operational transients and instrumentation errors. In additon, for plants presently near completion, it has been found that inserted rod hot channel factors do not even exceed the design hot channel factors.

Since the consequences of a dynamic rod drop are tolerable, the following discussion of rod drop protection is somewhat academic.

Rod drop protection diversity has been provided, both in the means of detection and in the means of actuating protection. Redundancy was more readily obtained by diverse instrumentation than by independent, but identical, channels. A rod drop signal is generated by either of the following:

a) A rapid decrease in indicated nuclear flux from any one of the four power range nuclear instrument channels

b) Rod bottom indication from any one of the rod position indicators when the associated rod bank is not on the bottom.

One-out-of-four logic for the nuclear channels is used because it was not known whether more than one channel would respond to the dropped rod. Therefore, redundancy is not claimed.

Protective action is directed toward inhibiting those mechanisms which would otherwise cause the reactor to return to its initial power level, i.e., automatic rod withdrawal and load demand with a negative moderator temperature coefficient. Again, since the magnitude of the hot channel factor increase was not known, it was assumed that both mechanisms would have to be inhibited.

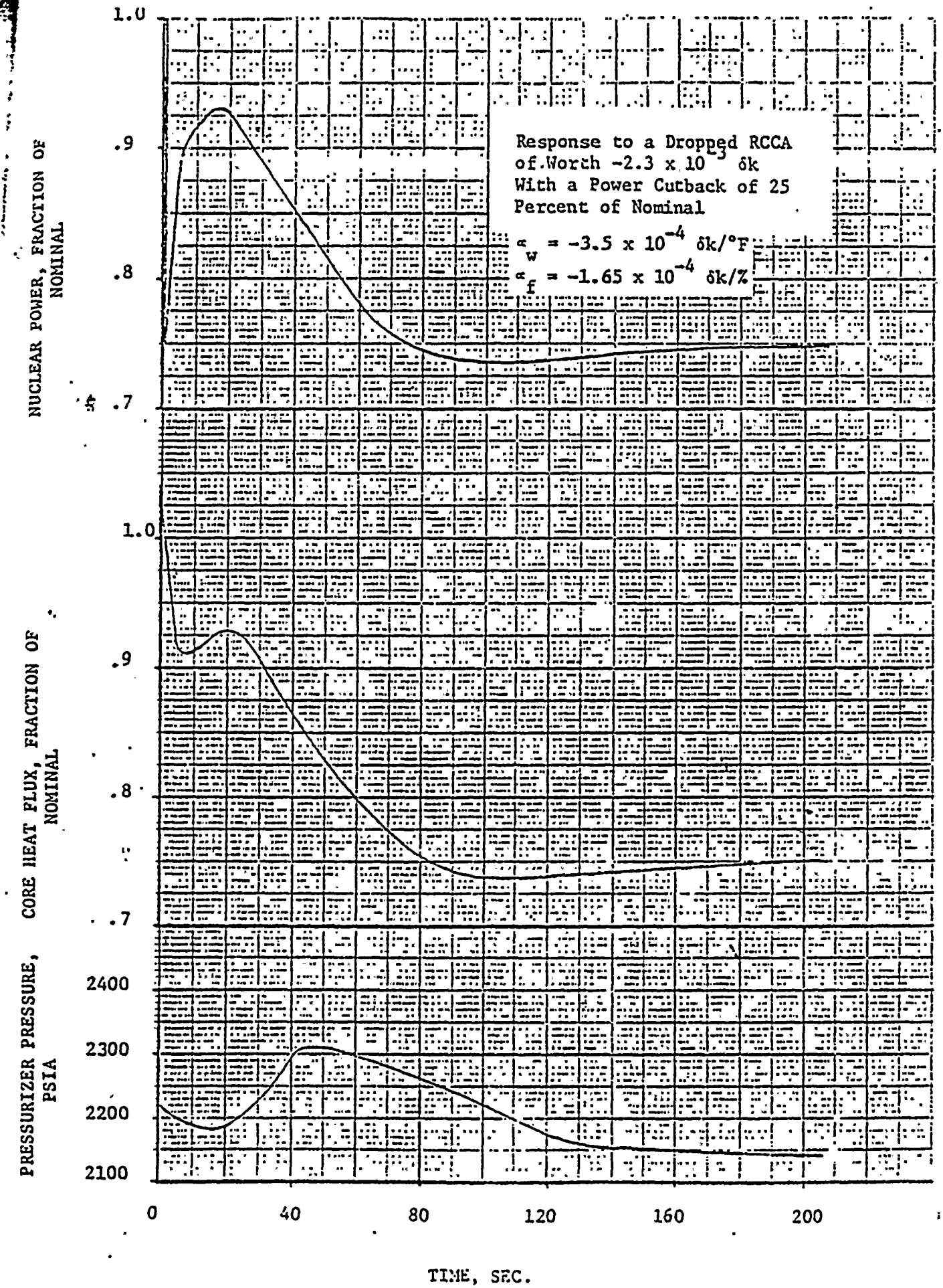
Redundant rod stop contacts are provided to block normal automatic control rod withdrawal. Manual rod withdrawal is not blocked since it is necessary to withdraw the dropped rod. Turbine load reduction is accomplished through redundant channels. Most plants are supplied with electro-hydraulic (E-H) control systems for the turbine. The turbine runback is activated by the following, either of which reduces or restricts turbine control valve position and steam load.

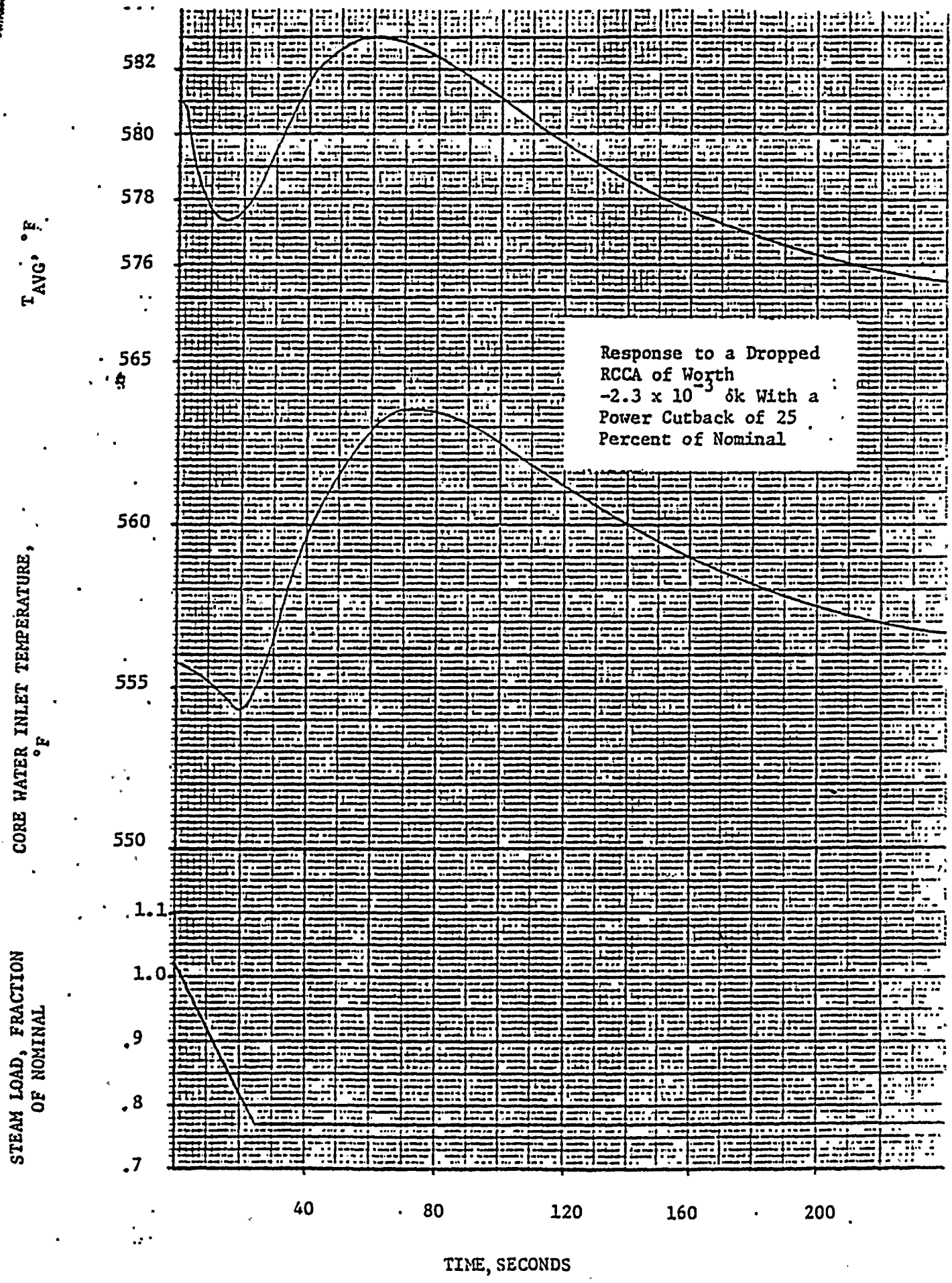
a) Reduction of the load reference setpoint of the turbine E-H controller by a preset amount. This is accomplished by reducing the set point at constant rate (200%/min.) for a preset time with a time delay relay.

b) Reduction of the turbine load limit to a preset value. The load limit (a clamp on the voltage signal controlling the turbine control valve position) is reduced until turbine thermal load as sensed by either of two turbine impulse pressure channels is below a preset value.

Following plant startup tests to verify that the DNB ratio is greater than 1.30 at full power with a dropped rod, it is intended to adjust the turbine runback for operational requirements. That is, the automatic load reduction would be large enough such that, with reasonable operator action, an orderly manual plant shutdown can be accomplished, rather than a reactor trip on low pressurizer pressure.

Figures 5.7-1 and 5.7-2 show the transient response of nuclear plant variables to a rod drop with turbine runback.


Response to a Dropped RCCA of Worth -2.3 x 10^-3 δk With a Power Cutback of 25 Percent of Nominal
α_w = -3.5 x 10^-4 δk/°F
α_f = -1.65 x 10^-4 δk/%
NUCLEAR POWER, FRACTION OF NOMINAL
CORE HEAT FLUX, FRACTION OF NOMINAL
PRESSURIZER PRESSURE, PSIA
1.0
.9
.8
.7
1.0
.9
.8
.7
2400
2300
2200
2100
0
40
80
120
160
200
TIME, SEC.


582
580
578
576
565
560
555
550
1.1
1.0
.9
.8
.7
T_{AVG}, °F
CORE WATER INLET TEMPERATURE, °F
STEAM LOAD, FRACTION OF NOMINAL
Response to a Dropped RCCA of Worth -2.3×10^{-3} δk With a Power Cutback of 25 Percent of Nominal
40
80
120
160
200
TIME, SECONDS

5.8 ENGINEERED SAFEGUARDS ACTUATION

Actuation of auxiliary feedwater is discussed in Section 5.2. Engineered safeguards for containment pressure protection are discussed in Section 5.9. Actuation of Emergency Core Cooling for loss of coolant protection is discussed in this section.

For loss of coolant protection, a safety injection signal is generated by either of two diverse sets of automatic signals:

a) Coincident low pressure and water level in the pressurizer;

b) High containment pressure.

Both sets of signals are redundant and meet all Protection System design criteria.

The signals derived from the pressurizer indicate that reactor coolant is being lost well before the core is uncovered. Reactor coolant blowdown also increases containment pressure. Set points for high containment pressure are typically about 10% of containment design pressure. This set point is reached well before the core uncovers.

Figure 5.8-1 shows the results of a calculation for a representative plant for the complete range of break sizes. It shows that either the pressurizer or the containment signal initiate safety injection 1-1/2 minutes or more before the core would be otherwise uncovered. (For large breaks, the passive accumulator system supplies water and delays the time at which active core cooling is required.) This analysis included the effects of containment heat sinks and fan coolers in delaying the time at which the containment high pressure signal is reached.

SAFETY INJECTION ACTUATION SIGNAL
VS
BREAK AREA

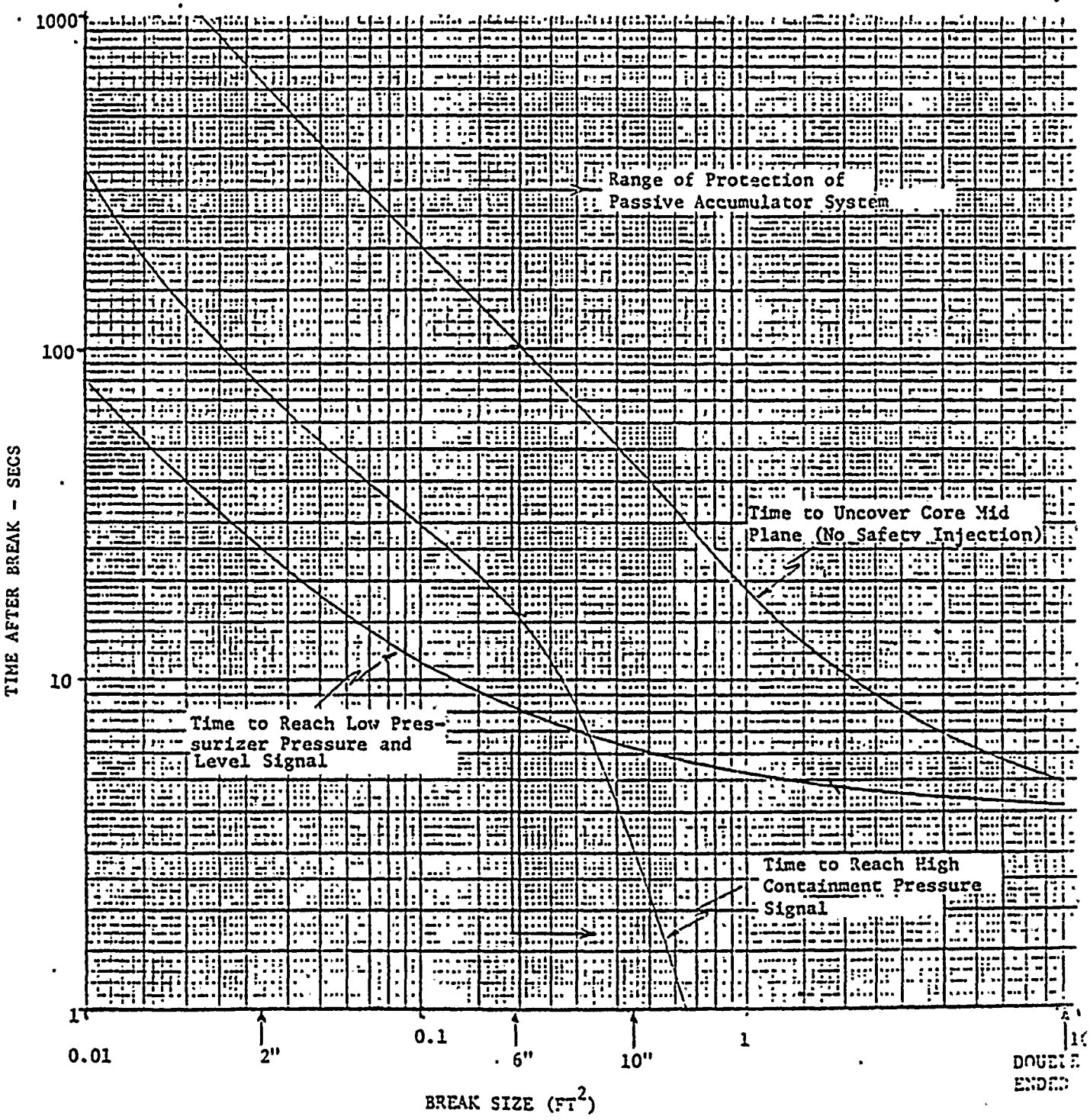


FIGURE 5.8-1

5.9 CONTAINMENT PRESSURE PROTECTION

Typical Westinghouse dry containment plants are equipped with fan cooler units and spray systems. These are provided to reduce the containment pressure to to essentially atmospheric following a loss of coolant accident or a steam line break accident inside the containment.

The containment is designed to withstand the total blowdown of the Reactor Coolant System or a steam generator with no dependence on the active safeguards. The active safeguards are, however, automatically actuated following the accident. The primary containment safeguards are the fan cooler units and their cooling water supply which are actuated by the safety injection signal which is generated by:

a) Coincident low pressurizer pressure and water level in the pressurizer

b) High containment pressure (approximately 10% of design pressure).

The backup containment safeguard, the containment Spray System, is actuated by a high containment pressure signal when the containment pressure reaches approximately 50% of the design value. Automatic spray actuation uses six containment pressure channels, in 2/3 _ 2/3 logic. The Spray System can also be actuated manually.

Only 2 out of 4 fan cooling units for two or three loop plants and 3 out of 5 cooling units for four loop plants are necessary to limit the containment pressure below design even considering that the Emergency Core Cooling System is unable to suppress boiling in the core, and the core decay heat energy continues to be added to the containment in the form of steam.

The operation of only one of the spray pumps is required in order for the Spray System to supplement the heat removal capability of the fan cooling units to provide a margin for effects from metal-water or other chemical reactions that could occur as a consequence of failure of Emergency Core Cooling Systems.

Since either fans or sprays are adequate, and diverse signals are used to actuate the fans, the Protection System is diverse for actuation of containment pressure protection.

5.10 EXCESSIVE LOAD

Excessive load is one means which could cause excessive core power generation. As distinct from the overpower-overtemperature accident discussed in Section 5.1 (Rod Withdrawal at Power), reactor coolant temperature, pressure, and pressurizer water level would not increase.

Reactor power follows turbine load, both by control design intent and the inherently negative moderator coefficient. An increase in load above design is therefore of potential concern.

Diverse overpower protection is provided by Reactor Protection System. These are the overpower delta-T and the nuclear overpower reactor trips. Since the accident is initiated from the secondary plant, the reactor coolant loop temperatures respond before the core coolant temperature. Piping lags applicable to the rod withdrawal accident are therefore not applicable to an excessive load accident, and either the delta-T or the nuclear overpower trip protects the core for any rate or magnitude load increase.

5.11 EXCESSIVE FEEDWATER FLOW

An excessive feedwater flow accident is primarily of concern to the turbine (high water level in the steam generator leads to excessive moisture carryover and potential turbine damage). With respect to nuclear protection, however, excessive feedwater flow (or feedwater temperature decrease) is seen as an excessive thermal load, and the discussion in Section 5.10 is applicable.

5.12 STATION BLACKOUT

A station blackout, or loss of all a-c power to the station auxiliaries, results from loss of incoming station a-c power coincident with a plant trip. Numerous reactor trip signals would be generated, such as turbine trip, low coolant flow, low feedwater flow, etc. This is not important however, since the loss of a-c power de-energizes the rod control power supply, and the control rods fall into the core, even if no reactor trip signal is generated.

Natural circulation of reactor coolant transfers reactor decay heat from the core to the steam generators. Since steam generator steam pressure is automatically controlled by the power-operated steam line relief valves (with backup from the steam line safety valves, if necessary), the only requirement for maintaining hot shutdown conditions is to supply feedwater to the steam generators.

The auxiliary feedwater system is discussed in Section 5.2, Loss of Feedwater. As noted in that section, the loss of a-c power starts all auxiliary pumps. A diverse automatic actuation signal - steam generator low water level - is also provided. Further, the energy sources for the auxiliary feedwater pumps are themselves diverse (steam-driven pumps and motor-driven pumps energized from the diesel-generator), such that failure to actuate an energy source does not prevent auxiliary feedwater.

5

APPENDIX

CONTROL AND PROTECTION FUNCTIONS

The reactor control and protection functions performed from each process parameter in the present Westinghouse design are tabulated below. Protection functions are listed first, and control functions listed last. Many functions; e.g., indication, alarms and interlocks, are not clearly either control or protection. These are classified as "supervisory" functions.

In the left margin, all functions are listed as P, S or C, showing protection, supervisory or control.

1. NUCLEAR INSTRUMENTATION

   1.1 Power Range
   1.2 Intermediate Range
   1.3 Source Range

2. REACTOR COOLANT SYSTEM PARAMETERS

   2.1 Reactor Coolant Temperature (ΔT, T_{avg})
   2.2 Pressurizer Pressure
   2.3 Pressurizer Water Level
   2.4 Reactor Coolant Flow

3. STEAM GENERATOR PARAMETERS

   3.1 Steam Generator Water Level
   3.2 Feedwater Flow
   3.3 Steam Flow
   3.4 Steam Line Pressure
   3.5 Steam Header Pressure

4. TURBINE PARAMETERS

4.1 Turbine First Stage Steam Pressure

4.2 Turbine Auto Stop Oil Pressure

4.3 Turbine Stop Valve Position

5. CONTROL ROD POSITION

5.1 Bank Position

5.2 Individual Rod Position

6. CONTAINMENT PRESSURE

7. ELECTRICAL PARAMETERS

7.1 Reactor Coolant Pump Bus

7.2 Reactor Coolant Pump Breaker Position

7.3 Feedwater Pump Power

1. NUCLEAR INSTRUMENTATION SYSTEM

1.1 Power Range - (linear indication in power range of operation).

P 1. Overpower reactor trip (high range) - rapid detection of fast overpower excursions during power operation.

P 2. Overpower reactor trip (low range) - protection during low power plant operation.

P 3. Top-to-bottom flux tilt bias of ΔT reactor trip set points - reduce DNB protection limits to offset effects of hot channel factors. (Both high ΔT reactor trips), see 2.1, 1&3

P 4. Reactor trip permissives

a. Permit single loop loss of flow trip at high power.
b. Permit reactor trip on turbine trip at high power.
c. Permit "at-power" trips during power operation.
d. Defeat manual block of low range and intermediate range overpower trips at low power.
e. Lock out source range high voltage supply during power operation.

S 5. Rod drop detection - rod stop and turbine runback to maintain DNB margins.

S 6. Overpower rod stop - stop a power excursion caused by rod withdrawal.

S 7. Overpower alarm (for equipment purposes, this function is combined with the overpower rod stop).

S 8. Control room indication and recording (including top-to-bottom difference).

S 9. Channel deviation alarm - detect channel failure, detect flux tilts.

S 10. Top-to-bottom flux tilt bias of ΔT rod stop and turbine runback set points (see 2.1, 2&4).

C 11. Automatic control rod motion - provide stable reactor control and rapid response.

1.2 Intermediate Range - (logarithmic scale for power range and upper startup range)

P 1. High level reactor trip - prevent power increase into power range unless power range channels are indicating.

P 2. Defeat manual block of source range high level trip - low intermediate range indication rearms source range trip.

S 3. High level rod stop - prevents excessive withdrawal of control rods during low power operation.

S 4. Control room indicating and recording.

S 5. Startup rate indication.

1.3 Source Range - logarithmic scale in shutdown range.

P 1. High level reactor trip - prevent startup accident from source range; prevent power increase into intermediate range unless intermediate range channels are indicating.

S 2. High count rate alarms - warn of approach to criticality.

S 3. Control room indication and audible count range.

S 4. Startup rate indication.

2. REACTOR COOLANT SYSTEM PARAMETERS

2.1 Reactor Coolant Temperature (ΔT-T_{avg})

P 1. Overtemperature high ΔT reactor trip - prevent core DNB (set point calculated from T_{avg}, pressure, and nuclear flux axial tilt).

S 2. Overtemperature high ΔT rod stop and turbine cutback - maintain operating margin to DNB (set point is a fixed margin below reactor trip set point).

P 3. Overpower high ΔT reactor trip - prevent high power density (set point calculated from nuclear flux tilt).

S 4. Overpower high ΔT rod stop and turbine runback - maintain operating power density (set point is a fixed margin below reactor trip set point).

S 5. Channel deviation alarms - detect channel failures, detect abnormal process conditions.

S 6. Control room indication and recording.

S 7. Control rod insertion limit alarm - maintain reactivity shutdown margin; maintain low ejected rod worth; maintain uniform core burnup.

In addition to the above functions for ΔT and T_{avg}, T_{avg} is also used for:

P 8. Low T_{avg} alarm (interlocked with high steam flow for steam line isolation) - steam break protection.

S 9. High T_{avg} alarm.

S 10. T_{avg} channel deviation rod stop (of automatic motion) - prevent spurious rod withdrawal or insertion.

S 11. T_{avg} deviation alarm - deviation from programmed setpoint.

C 12. Automatic control rod motion - control core power to maintain programmed temperature.

C 13. Steam dump control (condenser steam dump) - remove excess energy from reactor coolant.

C 14. Feedwater valve control - control addition to subcooled water to steam generators following a plant trip.

C 15. Pressurizer level programming - determine level setpoint to minimize charging and letdown changes during load changes.

2.2 Pressurizer Pressure

P 1. High pressure reactor trip - maintain pressure in ΔT protection range; provide overpressure backup to safety valves.

P 2. Low pressure reactor trip - maintain pressure in ΔT protection range.

P 3. Low pressure safeguards actuation - actuate loss of coolant protection.

P 4. High pressure defeat of safeguards actuation manual block - automatically remove manual block as operating pressure is approached.

P 5. Compensate overtemperature ΔT reactor trip setpoint - core DNB protection.

S 6. Compensate overtemperature T rod stop and turbine runback setpoint - maintain operating margin to DNB.

S 7. Control room indication and recording.

S 8. High-low pressure alarms.

S 9. Low pressure relief valve interlock - close relief valves on low pressure to avoid accidental loss of coolant.

S 10. Pressure control (on-off heaters, variable heaters, spray, and relief valve actuation) - maintain normal operating pressure.

C 11. Compensation signal for automatic control rod motion - improve reactor control response.

2.3 Pressurizer Water Level - (This variable measures reactor coolant fluid inventory and mean temperature).

P 1. High level reactor trip - prevent water discharge (an relief piping damage) through safety valves following rapid insurge.

P 2. Low level safeguards actuation - indication of loss of reactor coolant.

S 3. Control room indication and recording.

S 4. High-low level alarms.

S 5. Low level heater cutoff - prevent energizing heaters when uncovered (equipment protection).

S 6. Low level letdown isolation - prevent loss of coolant by excessive letdown.

S 7. High-low level deviation alarm - deviation from level set-point.

C 8. Charging pump speed control - maintain programmed water level.

C 9. High level deviation heater actuation - heat subcooled water insurge.

2.4 Reactor Coolant Flow

P 1. Low flow reactor trip - prevent core DNB.

S 2. Control room indication.

3. STEAM GENERATOR PARAMETERS

3.1 Steam Generator Water Level - (This variable is a measure of water inventory in steam generators).

P 1. Low-low water level reactor trip and auxiliary feedwater pump start - protect steam generators; preserve normal heat sink for removal of early decay heat.

P 2. Low level reactor trip (coincident with low feedwater flow) - provide rapid protection against a complete loss of feedwater flow.

S 3. High level feedwater control valve override - close feedwater valve to prevent excessive moisture carryover and turbine damage.

S 4. High-low level alarms.

S 5. Control room indication and recording.

S 6. Level deviation alarm - deviation from programmed level.

C 7. Feedwater valve control - maintain desired steam generator level.

3.2 Feedwater Flow

P 1. Low feedwater flow reactor trip (coincident with low steam generator water level) - provide rapid protection against complete loss of feedwater flow.

S 2. Control room indication and recording.

C 3. Feedwater valve control - provide stable control of steam generator level.

3.3 Steam Flow

P 1. Set point for low feedwater flow reactor trip (see 3.2.1 above).

P 2. High steam flow steam line isolation - steam break protection.

S 3. Control room indication and recording.

C 4. Feedwater valve control - provide rapid response of control for steam generator level.

3.4 Steam Line Pressure

P 1. Low pressure (or ~~low~~ high differential pressure) safeguards actuation - steam break protection.

P,C 2. Compensation of steam flow channels - provide accurate signal of steam flow.

S 3. Low steam pressure alarm.

S 4. Control room indication and recording.

C 5. Control of steam line relief valves - minimize actuation of safety valves.

3.5 Steam Header Pressure

C 1. Control steam dump to condenser.

S 2. Control room indication.

4. TURBINE PARAMETERS

4.1 Turbine First Stage Steam Pressure - (This variable is proportional to turbine steam load).

P 1. Reactor trip permissives - permits "at-power" reactor trips above minimum turbine load.

P 2. Steam line isolation - determines set point for high steam flow for steam break protection.

S 3. Control room indication.

S 4. Low power block of automatic control rod withdrawal - prevents unstable reactor control.

S 5. Steam dump interlock - prevents operation of steam dump to condenser unless a rapid loss of load has occurred.

C 6. T_{avg} program - determines set point for T_{avg} in control rod and steam bypass control systems.

C 7. Steam generator level program - determine set point for level in feedwater control system.

4.2 Turbine Auto-Stop Oil Pressure - (Presence or absence of oil pressure indicates trip or non-trip condition of turbine).

P 1. Reactor trip - prevent temperature-pressure excursion in reactor coolant from loss of steam load.

C 2. Steam bypass control - selects mode of control.

C 3. Feedwater control - selects mode of control, steam generator water level or T_{avg}.

? 4.3 Turbine Stop Valve Position - used as backup to autostop oil pressure for reactor trip signal.

5. CONTROL ROD POSITION

5.1 Bank Position - (Step counters)

S 1. Bank insertion limit alarm (set point determined from T_{avg} and ΔT) - maintain reactivity shutdown margins; maintain acceptable core power distribution.

S 2. Bank withdrawal limit alarm - warn operator that control rods are nearing the end of their useful travel.

S 3. Control room indication and recording.

5.2 Individual Rod Position - (LVDT)

S 1. Rod position deviation alarm - warn of possible rod malpositioning.

S 2. Rod bottom rod drop detection - rod stop and turbine runback to maintain DNB margins.

S 3. Control room indication and recording.

6. CONTAINMENT PRESSURE

P 1. High containment pressure safeguards actuation and reactor trip - protection against small steam breaks, backup protection for loss of coolant accidents and large steam breaks.

P 2. High containment pressure steam line isolation.

P 3. High containment pressure spray actuation.

S 4. Control room indication.

7. ELECTRICAL SYSTEM VARIABLES

7.1 Reactor Coolant Pump Bus

P 1. Undervoltage reactor trip - protection against multi-loop loss of flow.

P 2. Underfrequency reactor trip and RCP breaker opening - prevent rapid system frequency opening - prevent rapid system frequency decrease from braking RCP.

7.2 Reactor Coolant Pump Breaker Position (contacts)

P 1. Reactor trip on breaker opening - backup to low flow protection for loss of flow.

7.3 Feedwater Pump Power

P 1. Auxiliary feedwater system actuation (feedwater pump breaker position and/or bus voltage) - backup feedwater protection for loss of feedwater.

ATTACHMENT 8 TO AEP:NRC:1184H2

RESPONSE TO ITEM 8

DEFENSE-IN-DEPTH EVALUATION PERFORMED FOR THE REACTOR PROTECTION AND CONTROL PROCESS INSTRUMENTATION REPLACEMENT PROJECT