Westinghouse Systems Course
R-304P

Day	Title	Chapter or Location
1 (Tuesday)	TTC Introduction PWR Systems Overview Core Characteristics	Classroom 1.2 2.1
2 (Wednesday)	Simulator Review Core and Vessel Construction Reactor Coolant System	Simulator 3.1 3.2
3 (Thursday)	Simulator Review Primary Instrumentation CVCS & Pressurizer Level Control	Simulator 10.1 & 10.2 4 & 10.3
4 (Friday)	Simulator Review Main and Auxiliary Steam Main Turbine and Auxiliaries Condensate and Feedwater Steam Generator Water Level Control	Simulator 7.1 7.3 7.2 11.1
5 (Monday)	Simulator Review Steam Dump Control EHC and MSR Control	Simulator 11.2 11.3 & 11.4
6 (Tuesday)	Mini Quiz Simulator Review Cooling Water Systems Excore Nuclear Instrumentation	Classroom Simulator 14.1-14.4 9.1
7 (Wednesday)	Simulator Review Incore Instrumentation Rod Control System	Simulator 9.2 8.1
8 (Thursday)	Mini Quiz Simulator Review Power Distribution Limits Rod Position Indication Rod Insertion Limit	Classroom Simulator 2.2 8.2 & 8.3 8.4
9 (Friday)	Simulator Review Reactor Trips and ESF Actuation Signals RPS Design and Testing	Simulator 12.2 & 12.3 12.1
10 (Monday)	Simulator Review Intro to ESF Systems Residual Heat Removal System Emergency Core Cooling Systems	Simulator 5.0 5.1 5.2
11 (Tuesday)	Mini Quiz Simulator Review Auxiliary Feedwater System Electrical Distribution	Classroom Simulator 5.8 6.0
12 (Wednesday)	Simulator Review Containment and Containment Systems Fuel Handling and Storage	Simulator 5.3-5.6 17

13 (Thursday)	Simulator Review Plant Commuter Radiation Monitoring Plant Operations	Simulator 18 16 19
14 (Friday)	Final Examination	Classroom

of coolant accident, the function of the RHR is to provide cool, borated water from the Refueling Water Storage Tank (RWST) to the RCS for the short term and recycle fluid from the containment building sump back into the reactor coolant system for long term cooling.

The Safety Injection (SI) System is another emergency core cooling system located in the auxiliary building. It's function is to inject borated water from the RWST into the RCS after a LOCA. Although the SI system discharge capacity is much less than that of the RHR, it's discharge pressure is greater.

The Chemical and Volume Control System (CVCS) maintains the purity of the reactor coolant by means of demineralizer beds that continuously purify a small letdown stream from the RCS. This purified water is charged back into the RCS at a controlled rate to maintain the proper volume of water in the RCS. The CVCS charging pumps also serve as the high pressure safety injection pumps. Their function is to supply borated water to the RCS in emergency situations.

In the event of a LOCA, the hot reactor coolant spills from the RCS into the containment and flashes to steam. This action causes a pressure increase inside the Containment Building.

The containment spray system is designed to transfer water from the refueling water storage tank to spray rings located high inside containment. The cool water spraying into the containment, quenches the steam and maintains the pressure inside of the containment to within design limits. This prevents rupture of the containment building and the subsequent uncontrolled release of radioactive materials to the environment.

The Component Cooling Water System (CCW) provides a cooling medium to various components such as the CVCS letdown heat exchanger and the RHR heat exchanger. This system (CCW) is a closed loop system and is cooled by the Service Water System (SWS) which receives its water from a river, lake or ocean. Both of these systems (CCW and SWS) are safety systems and are required to function in order to mitigate the consequences of analyzed accidents.

1.2.5 Plant Layout (Figure 1.2-2)

The entire RCS, including the steam generators, is located within the containment building. This structure isolates the radioactive reactor coolant from the environment in the event of a leak or a loss of coolant accident. The containment building is designed to withstand the pressure produced by a complete rupture of the largest pipe of the reactor coolant system. In addition, the containment must be able to perform this safety function during and following a "design basis earthquake".* The containment building is therefore designated as a Seismic Category I structure.

* A "design basis earthquake" is also called a "safe shutdown earthquake" and is defined in 10CFR part100 Appendix A of the Code of Federal Regulations. Paraphrasing this part of the code - a design basis earthquake is the maximum ground motion potential considering local and regional geology and seismology. It is that earthquake which produces the maximum vibratory ground motion for which certain structures, systems, and components are designed to remain functional. "Safety related" systems, structures and components designed to remain functional during a design basis earthquake are designated "Seismic Category I".

Safety-related and potentially radioactive auxiliary systems are located inside the Seismic Category I auxiliary building. This building is normally located between the turbine building and the containment building. Ventilation from the auxiliary building is passed through high efficiency particulate filters and/or charcoal filters to minimize the release of radioactive material to the environment. A fuel storage building (sometimes a part of the auxiliary building) is provided for handling and storage of new and spent reactor fuel. The fuel storage building is also designated as a Seismic Category I building. The control building (also sometimes part of the auxiliary building) is a Seismic Category I structure, housing the main control room, the cable spreading room, auxiliary instrument room, plant computer and battery rooms.

The turbine building is not "safety related" and contains most of the secondary cycle equipment and secondary support systems. The main turbine, moisture-separator/reheaters, main condenser, condensate and feedwater pumps, and feedwater heaters, are all located inside the turbine building.

1.2.6 Plant Control

The power output of the reactor and the outlet temperature of the coolant from the reactor core is controlled by manipulating several factors which affect the core's reactivity (neutron production capability). The position of neutron absorbing control rods, the concentration of boric acid in the RCS and the steam flow rate can be changed to affect reactor power and its outlet temperature..

The automatic control systems are designed to provide power change (load change) capability between 15% and 100% of rated power at 5% per minute (ramp) or a 10% instantaneous (step) change in power without causing an automatic reactor shutdown (trip). Additionally, the plant's steam dump system is designed to direct steam to the main condenser allowing the unit to accept a large power reduction (load rejection) without tripping the reactor.

The power level of the reactor is normally changed by selecting a desired electrical load and load rate via the turbine control system and allowing the reactor to follow the turbine load change. Various methods are possible for controlling the reactor's power, as the turbine load is changed, and are discussed below.

1.2.7 Reactor Control

The basic formula defining heat (or power) transferred across a heat exchanger (in this case, the steam generators) is:

$$Q = UA\Delta T$$

where:

Q = heat transferred in BTU's
U = heat transfer coefficient
A = area of heat transfer
ΔT = differential temperature across the heat exchanger or as in this case the difference between the average temperature of the reactor coolant (T_{avg}) and the temperature of the steam (T_{stm}).

For all practical purposes, both the heat transfer coefficient (U), and the heat transfer area (A), are assumed to be constant. Since the heat transfer coefficient is a function of the materials used in the construction of the steam generator and the U-tubes are covered with water. The equation may be reduced to:

$$Q \propto \Delta T$$

or

$$Q \propto T_{avg} - T_{stm}$$

There are three basic modes of reactor coolant detail in the following paragraphs.

In reactor operation, K_{eff} is the most significant property with regard to reactor control. At any specific power level or condition of the reactor, K_{eff} is kept as near to the value of 1.0 as possible. At this point in operation, the neutron balance is kept to exactly one neutron completing the life cycle for each original neutron absorbed in the fuel. An example of this balance is shown in Table 2.1-3.

The operational factors that affect reactor control are all-important because of the way they change the factors that make up K_{eff}. As seen in the previous table if any one of these factors making up K_{eff} changes, the the ratio of 1.0 will not be maintained. This resultant change in K_{eff} will either make the reactor subcritical or supercritical.

2.1.5.1 Fast Fission Factor

The fast fission factor, ε, is the contribution to neutron multiplication from the fissions that occur at higher-than-thermal energies. This contribution is from the fast fission in U-235 and U-238. The probability for a fission reaction in U-238 is relatively low, but there is so much of this isotope in the reactor core that there is a contribution to the multiplication factor. The fast fission factor is defined as the ratio of the neutrons produced by fissions at all energies to the number of neutrons produced in thermal fission. As core temperature is increased, the value of e is increased because more fast neutrons are present to fission the U-238 due to poorer moderating properties of the water. There is only a slight, almost insignificant, change over the core lifetime due to loss of U-238 by conversion to Pu-239.

2.1.5.2 Fast Nonleakage Factor

The fast nonleakage factor, L_f, is the fraction of neutrons that is not lost due to leakage from the core system during the slowing down process from fission energies to thermal energies. It is also the probability that a neutron will remain in the core and become a thermal neutron without being lost by fast leakage. It is represented by:

$$L_f = e^{-\tau B^2}$$

for the continuous slowing down model, or by:

$$L_f = \frac{1}{1+\tau B^2}$$

for the two-group model. "Two-group" indicates that the core can be described as consisting of only thermal and one representative group of fast, or epithermal, neutrons. Fermi age, τ, is a measure of how far fast neutrons travel before being thermalized. B^2 is called buckling and depends on the shape and size of the core. Small cores have larger buckling than large cores.

As the temperature of the core increases, L_f decreases because of the increase in the numerical value of τ from the decreasing density of the water. The change during core life is almost insignificant because it is primarily due to a change in metal-to-water ratio, which is constant with core age.

2.1.5.3 Resonance Escape Probability

The resonance escape probability, symbolized by p, is the probability that a neutron will be slowed to thermal energy and will escape resonance capture. It is also the fraction of neutrons that escape capture during the slowing-down process. It is always less than 1.0 when there is any amount of U-238 or Pu-240 present in the core, which means that high-energy capture by these isotopes always removes some of the neutrons from the neutron life cycle.

As the reactor temperature increases, the resonance escape probability decreases in value because of the decrease in the ratio of the water-moderating atoms to fuel atoms and the broadening of the resonance capture cross sections. The resonance escape probability increases with core lifetime due to the decrease in fuel temperature. These changes in the resonance escape probability will be discussed further in Section 2.1.6.1, "Fuel Temperature Coefficient".

2.1.5.4 Thermal Nonleakage Factor

The thermal nonleakage factor, L_t, is the fraction of the thermal neutrons that do not leak out of the core during thermal diffusion but remain to contribute to the chain reaction. L_t is also the probability that a thermal neutron will remain and be utilized in the core. It is a calculated value for each condition of the core and is represented by the equation:

$$L_t = \frac{1}{1+L^2B^2}$$

where L^2 is the thermal diffusion length squared and B^2 is the geometric buckling of the system. The value of L_t decreases as the temperature of the core increases; the effect can be seen from the value of L^2, which is a measure of how far thermal neutrons travel before absorption. When temperature is increased, the values of all absorption cross sections decrease. This increases L^2, which in turn decreases L_t. Buckling [B^2] does not change over the range of interest. As the core is operated and fuel is consumed, the value of L_t decreases as a result of fuel burnup.

2.1.5.5 Thermal Utilization Factor

The thermal utilization factor, f, is the ratio of the probability that a neutron will be absorbed in the fuel to the probability that the neutron will be absorbed in all the material that makes up the core. This factor is the one that the plant operator has the greatest control over. It is described by the following equation:

$$f = \frac{\Sigma_a(fuel)}{\Sigma_a(fuel)+\Sigma_a(other)}$$

where Σ_a= macroscopic absorption cross section, which is the sum of the capture cross section, Σ_c, and the fission cross section, Σ_f.

$$\Sigma_a = \Sigma_c + \Sigma_f$$

An examination of the thermal utilization factor shows that the Σ_a (fuel) comprises only the absorption by the U-235 at the beginning of core life. As the amount of Pu-239 increases because of the irradiation of U-238 in the core, it is necessary to consider the change of fuel concentration in determining the value of f at different times in the core lifetime. The reactor operator can change Σ_aã(other) by positioning of the control rods and by addition or removal of boric acid from the moderator.

2.1.5.6 Neutron Production Factor

The neutron production factor, η, is the average number of neutrons produced per thermal neutron absorbed in the fuel. It is based on physical measurement for each type of fuel used in a reactor.

The numerical value of η does not change with core temperature over the range considered for most reactors. There is essentially no change in η over the lifetime of the reactor core because the values for U-235 and Pu-239 are very close. As the reactor operates, and Pu-239 begins to contribute to the neutron economy of the core, the average effect on η is expressed by:

$$\eta = \frac{(\nu\Sigma_f)^{235}+(\nu\Sigma_f)^{239}}{\Sigma_a^{235}+\Sigma_a^{238}+\Sigma_a^{239}}$$

(reciprocating) pump equipped with variable speed drive. The positive displacement pump is powered from a non-vital ac source. All parts in contact with the reactor coolant are fabricated of austenitic stainless steel or other materials of adequate corrosion resistance. The centrifugal pump seals and the reciprocating pump stuffing box are provided with leak offs to collect reactor coolant leakage before it can escape to the atmosphere. There is a minimum flow recirculation line for the centrifugal charging pumps to protect them from a low flow condition. The reciprocating pump has a recirculation line and a relief valve to the VCT for over pressure protection.

The charging flow rate is determined by the pressurizer level control system. Control of the flow rate from the reciprocating pump is accomplished by varying the speed of the pump. With a centrifugal charging pump operating, the charging flow rate is controlled by varying the position of a modulating valve (FCV-121) on the discharge of the centrifugal pumps. The charging flow measured downstream of FCV-121 (by FT-121) is an input to the controller which positions the valve (see Chapter 10.3).

The centrifugal charging pumps also serve as the high head safety injection pumps in the emergency core cooling system.

RCP Seal Flow Control Valve

The reactor coolant pump seal flow control valve (HCV-182), located in the charging header, determines the division of flow between the RCP seal injection path and the charging flow path. This valve is remotely adjusted by the control room operator. RCP seal flow is increased by throttling closed HCV-182. If seal flow is increased, then the charging flow is decreased. Conversely, if HCV-182 is throttled open, the seal flow decreases and the charging flow increases.

Charging Isolation Valves

Two series, motor-operated isolation valves, (MO-8105 and MO-8106) isolate the charging header on an engineered safety features actuation signal.

Two charging paths to the RCS are provided. The normal path is into loop 1 through an air operated isolation valve, (CV-8146). A spring loaded check valve set to open at 200 psid is in parallel with the isolation valve. The purpose of this spring loaded check valve is to relieve the volumetric expansion of coolant if charging were to be isolated and letdown continued. The alternate charging connection (CV-8147) taps into loop 4, and can be used if the normal charging line is inoperable.

Pressurizer Auxiliary Spray

The charging header can supply spray to the pressurizer if the reactor coolant pumps are not running. Depressurization while on residual heat removal is a normal evolution requiring the use of the auxiliary spray valve.

The auxiliary spray line is routed from the outlet of the regenerative heat exchanger to the pressurizer spray line downstream of the normal pressurizer spray valves. Auxiliary spray flow is controlled by a remotely controlled air operated valve (CV-8145).

4.1.3.4 Seal Injection and Seal Return

Seal Injection Header

The reactor coolant pump seal injection header connects to the CVCS at the discharge of the charging pumps, and directs flow to the seal injection filter(s). The seal injection filters are 5 micron filters installed to collect particulate matter that could damage the reactor coolant pump seal faces. The filtered seal injection water is directed to each reactor coolant pump through individual injection lines.

A total seal injection flow of 32 gpm, controlled by the seal injection flow control valve (HCV-182), is divided equally among the four reactor coolant pumps. Each seal injection line contains a manual throttle valve, locked in a throttled position, used to balance pump seal injection flow rates, and a manually operated isolation valve.

Seal Return Header

A seal return flow of 3 gpm/RCP is returned to the CVCS. The individual pump seal return lines join together and exit the containment through one penetration. Motor operated isolation valves (MO-8112 and MO-8100), located on opposite sides of the containment building penetration, provide redundant isolation of the seal return line should a containment phase "A" isolation occur. A relief valve, located in the containment, routes seal return flow to the pressurizer relief tank (PRT) if the seal return motor operated isolation valves are closed. The relief valve lifts at 150 psig.

A filter is installed in the seal return piping to collect particulates from the seal return and excess letdown systems. The filtered seal return water passes through the seal water heat exchanger to the charging pump suction header.

The seal water heat exchanger is also used to cool the centrifugal charging pump recirculation flow. This heat exchanger is cooled by the component cooling water system.

4.1.3.5 Excess Letdown

Excess letdown Figure 4.1-1 is supplied from the loop 3 cold leg through excess letdown heat exchanger and isolation valves to the CVCS.

Excess Letdown Control Valves

Four remotely-operated valves are associated with the Excess Letdown System. Two valves (FCV- 8153, and 8154) are located on the excess letdown heat exchanger inlet. A valve (HCV-123) on the excess letdown heat exchanger outlet is positioned by a hand controller in the control room, and is used to throttle excess letdown flow. A three way valve (CV-8143) is used to direct excess letdown flow to the CVCS or to the reactor coolant drain tank (RCDT). Excess letdown flow is normally routed to the CVCS.

Excess Letdown Heat Exchanger

The excess letdown heat exchanger cools reactor coolant letdown flow and has a capacity, at full system operating pressure equal to that portion of the seal injection flow which enters into the RCS through the reactor coolant pump labyrinth seals (normally, 20 gpm).

The excess letdown heat exchanger can be employed either when normal letdown is temporarily out of service to maintain the reactor in operation or it can be used to supplement maximum letdown during the final stages of heatup. The letdown fluid flows through the tube side of the excess letdown heat exchanger and component cooling water is circulated through the shell.

4.1.4 System Features and Interrelations

4.1.4.1 Deborating Ion Exchangers

Some Westinghouse plants are equipped with deborating ion exchangers. Late in core life, the necessary boron concentration of the RCS approaches zero. At low boron concentrations, the volume of dilution required to further decrease

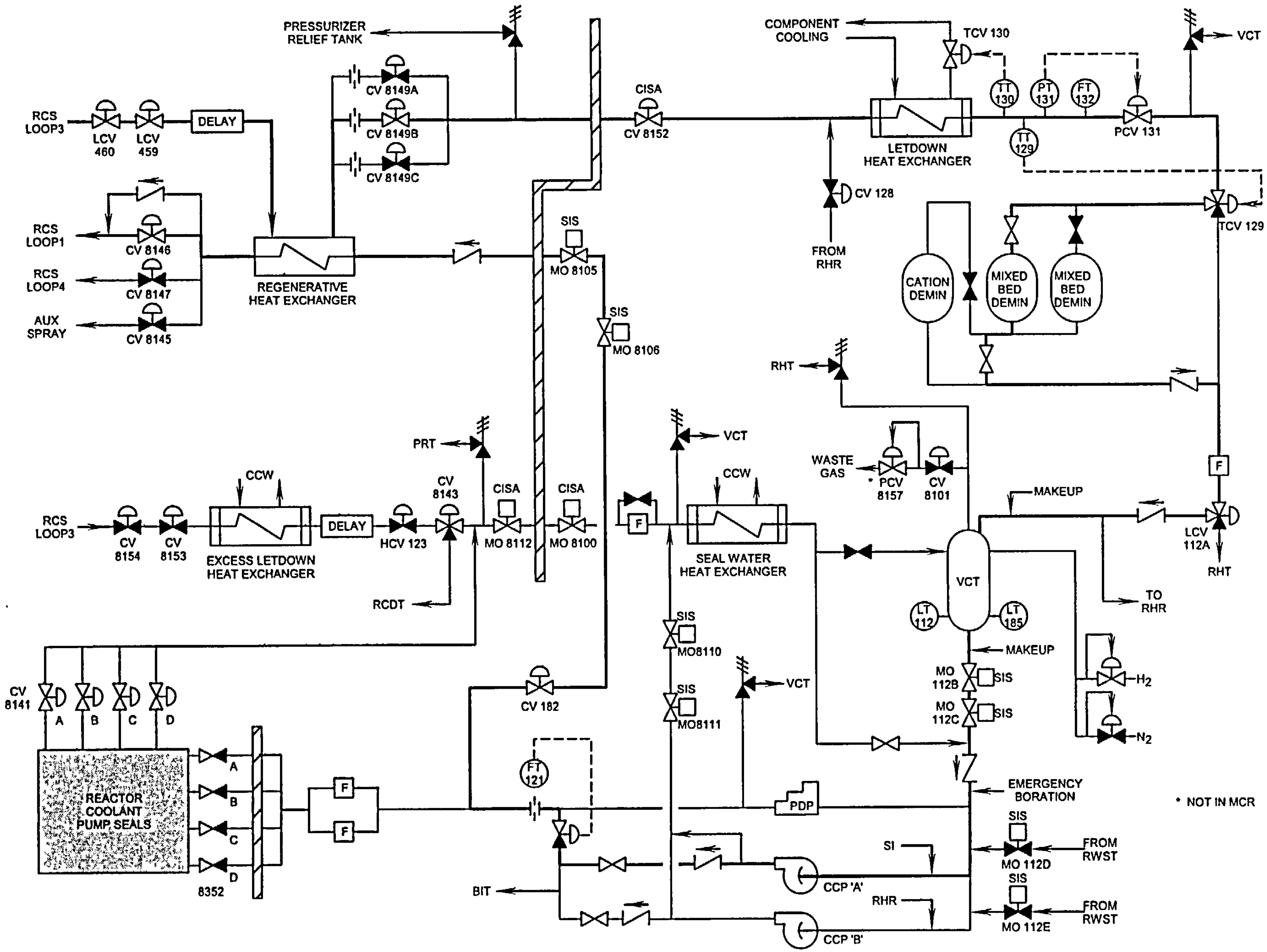


Figure 4.1-1 Chemical and Volume Control System

0202-356
2458-1

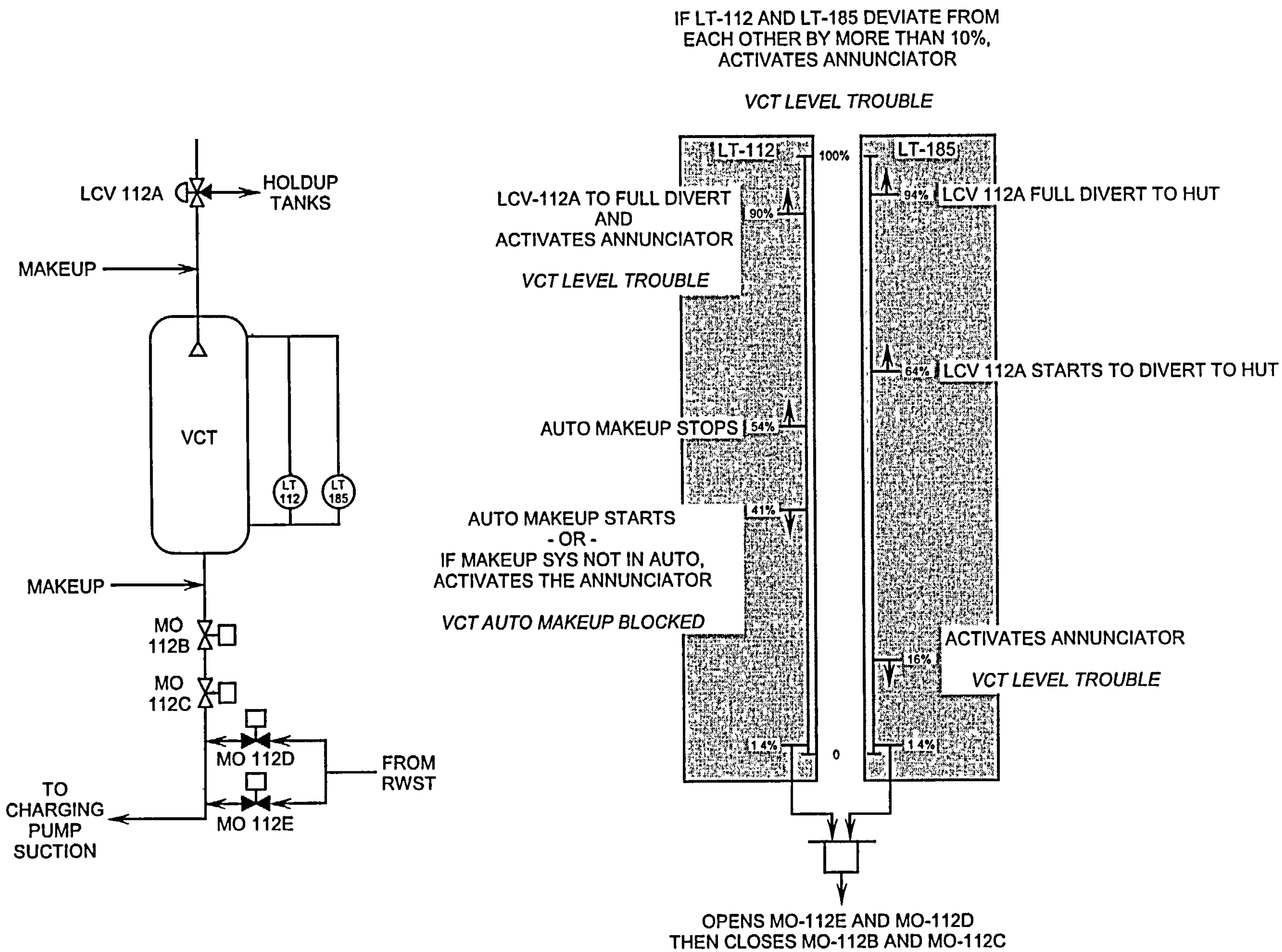
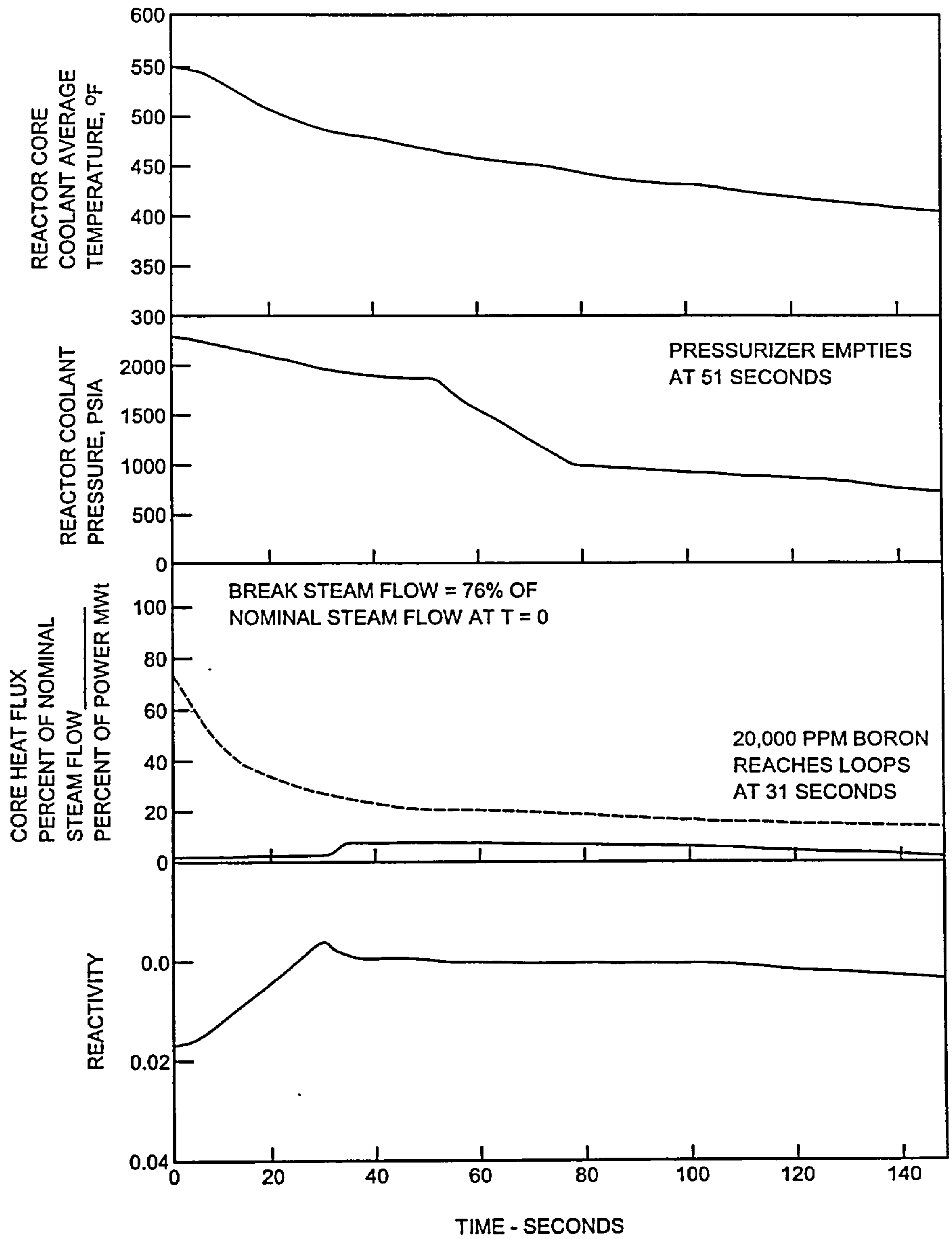


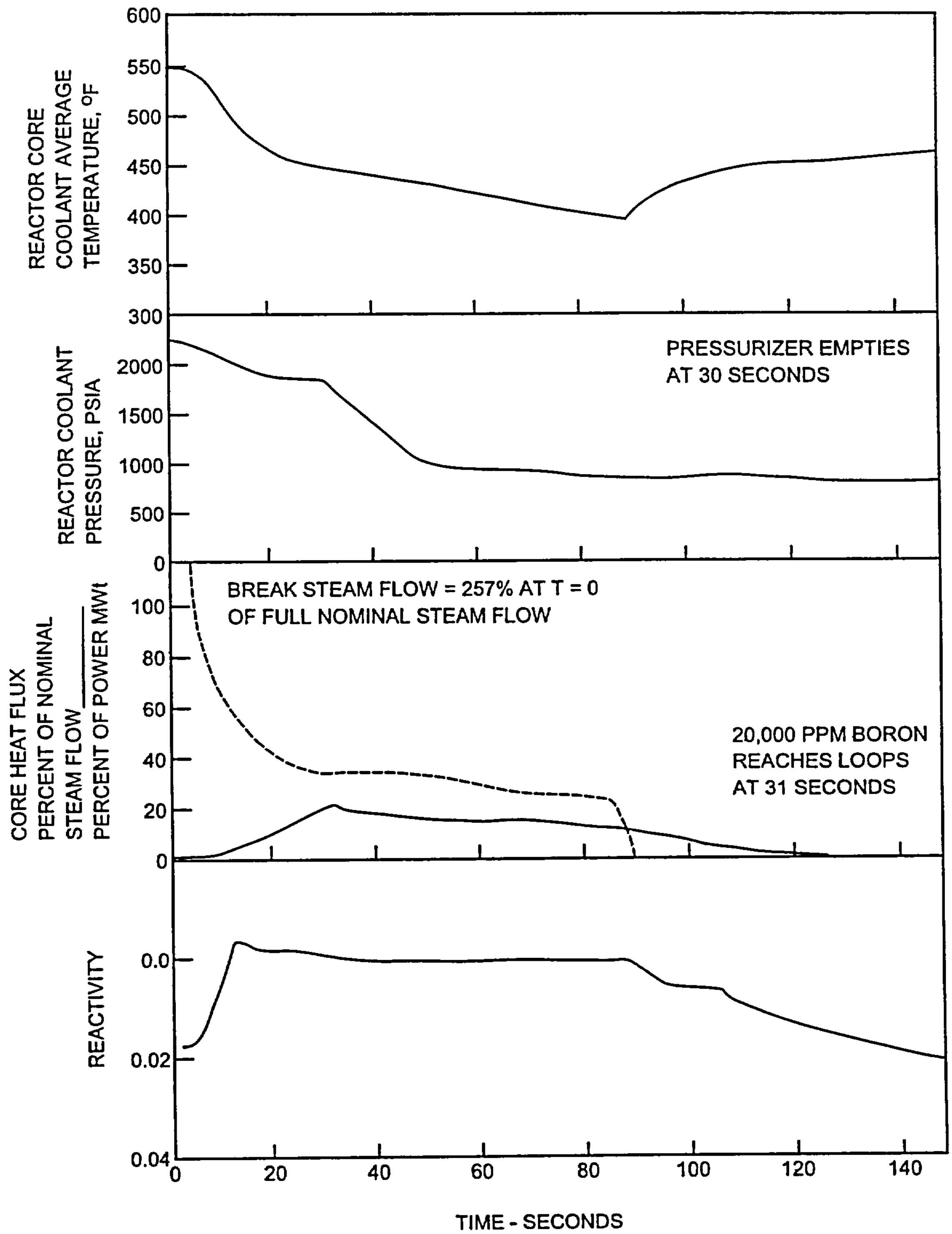
Figure 4.1-7 VCT Level Functions

0102-356
2 4 8-1



Safety Injection with Offsite Power

Figure 5.0-1 Steam Line Break Downstream of Flow Measuring Nozzle



Safety Injection with Offsite Power

Figure 5.0-2 Steam Line Break at Exit of Steam Generator

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

5.2.3.2 High Head Injection System

The high head injection system (Figure 5.2-3) includes the centrifugal charging pumps, which during normal plant operations supply charging flow in the chemical and volume control system (Chapter 4.1). Under accident conditions these pumps deliver water from the refueling water storage tank (Section 5.2.3.4) to the RCS at the prevailing RCS pressure. Each centrifugal charging pump is of the multistage, diffuser design, with a barrel-type casing and vertical suction and discharge nozzles. The unit has a self contained lubrication system and a mechanical seal cooling system. Component cooling water is the normal heat exchange medium. Pump design parameters are listed in Table 5.2-3.

A minimum flow bypass line is provided on each pump discharge to recirculate flow to the volume control tank after cooling in the seal water heat exchanger to protect the pumps at the shutoff head. The charging pumps may be tested during normal operation through the use of the minimum flow bypass line.

Receipt of an engineered safety features actuation signal will initiate the following actions in the high head injection system.

1. The centrifugal charging pumps will receive a start signal.
2. The suction valves from the volume control tank (112B, 112C) will close and the suction valves from the refueling water storage tank (112D, 112E) open. This provides a source of borated water to the suction of the pumps.
3. In order to limit the bypass flow around the boron injection tank the minimum flow recirculating valves (8110, 8111) close.
4. To establish a flowpath to the RCS the boron injection tank inlet (8803A&B) and outlet (8801A&B) valves open.

The high head injection system will continue to operate in this configuration until the lineup is changed by the reactor operator. The discharge pressure of the centrifugal charging pumps is sufficient to provide flow to the RCS for any postulated size break. Pump capacity and pressure capability allow the pumps to deliver flow under all pressure conditions up to and including pressurizer safety valve lift pressure.

A last-resort method of cooling the core known as bleed and feed can be used if heat transfer from the reactor coolant to the steam generators is unavailable. For this cooling method, flow through the core is delivered by the charging pumps and displaced out intentionally opened power-operated pressurizer relief valves.

5.2.3.3 Boron Injection Tank (BIT)

The boron injection tank is being phased out of use. At most Westinghouse units the function of the BIT has been eliminated; however, the tank might still remain in the high head injection flow path. Since some units might still incorporate the BIT into their designs, this section is provided to explain the design and function of this tank.

The BIT (Figure 5.2-3) contains a boric acid solution (2000 to 20000 ppm) and is connected to the discharge of the centrifugal charging pumps. Upon actuation of the safety injection signal, the charging pumps provide the pressure to inject the boric acid solution into the reactor coolant system when the isolation valves open. To prevent cold spots and stratification within the tank during normal operation, the contents of the BIT are continuously recirculated with boron injection recirculation pumps. These pumps are rated at 2 horsepower and provide a flow of 20 gpm. The recirculation flow path includes a 75-gal stainless steel surge tank, which accommodates volumetric changes in the system.

The boron injection tank incorporates a sparger type inlet which distributes the incoming boric acid in 360 degrees as it enters the tank. Redundant tank heaters and line heat tracing are provided to ensure that the solution will be stored at a temperature greater than the solubility limit of boric acid (normally greater than 135°F).

The design basis of the boron injection tank is to provide the negative reactivity needed to ensure the reactor remains subcritical even during the worst-case cooldown accident. This is the cooldown (and the associated positive reactivity addition) from a steam line break. Boron injection tank design parameters are listed in Table 5.2-4.

5.2.3.4 Refueling Water Storage Tank (Figure 5.2-1)

The refueling water storage tank is designed to hold enough borated water (borated to 2000 ppm), to fill the refueling cavity for refueling operations and to provide water for ECCS operation. The volume of the RWST is 438,000 gallons with a Technical Specification minimum volume of 428,000 gallons. The RWST is always aligned for safety injection operation to provide water for the centrifugal charging, safety injection, residual heat removal, and containment spray pumps.

The refueling water storage tank is protected from back flow of reactor coolant from the reactor coolant system. All connections to the refueling water storage tank are provided with check valves to prevent back flow. When the RCS is hot and pressurized there is no direct connection between the RWST and the RCS. When the reactor coolant system is being cooled down and the residual heat removal system is placed into operation, the RHR system is isolated from the RWST by a motor operated valve (8812) in addition to a check valve. RWST design parameters are listed in Table 5.2-5.

5.2.3.5 Intermediate Head (Safety Injection System)

The intermediate head injection system (Figure 5.2-4), also referred to as the safety injection system, utilizes two safety injection pumps. Each intermediate head safety injection pump is a multistage centrifugal pump. The pump is driven directly by an induction motor. The unit has a self contained lubrication system and mechanical seal cooling system. Component cooling water is the normal pump heat exchange medium.

A minimum flow bypass line is provided on each pump discharge to recirculate flow to the refueling water storage tank in the event the pumps are started with the normal flow paths blocked. This line also permits pump testing during normal operation. Two motor operated valves (8814& 8813) are provided in this line. These valves are closed by operator action during the recirculation mode.

The safety injection pump system is designed to provide water from the RWST to the four reactor coolant system cold or hot legs in the case of a relatively small break where the system pressure continues to remain high for a relatively long period.

The safety injection pump system is aligned during normal operations to perform its accident function. Upon receipt of an engineered safety features actuation signal, the pumps will start and recirculate to the RWST until RCS pressure decreases below pump discharge pressure. Initial injection is into the cold legs of the RCS. Injection into the RCS hot leg valves (8802A&8802B) is a manual realignment completed by the operator. Safety injection

5.4 CONTAINMENT TEMPERATURE, PRESSURE, AND COMBUSTIBLE GAS CONTROL

Learning Objectives:

1. State the purposes of the containment ventilation systems.
2. List the signals that automatically initiate purge and exhaust system isolation.
3. State the purposes of the containment spray system.
4. List the signals that automatically initiate the containment spray system.
5. State the purpose of the containment hydrogen recombiners.

5.4.1 Introduction

The purposes of the containment temperature, pressure, and combustible gas control systems are as follows:

1. To control the temperature and pressure of the containment during normal operations.
2. To protect the containment barrier and to minimize the leakage of radioactivity to the environment following an accident by reducing the containment temperature and pressure.
3. To remove hydrogen from the containment atmosphere to prevent explosive mixtures.
4. To remove radioactive iodine from the containment atmosphere after a LOCA.

The central safety objective in reactor plant design and operation is the control of the radioactive fission products. To ensure this objective is met, the containment must be designed and maintained so that the fission products are retained after operational and accidental releases inside the containment.

The containment temperature, pressure and combustible gas control systems are those systems which are necessary for reducing the release of airborne radioactivity and ensuring continued containment integrity. These containment systems function as necessary during normal operation and during the period following a postulated accident.

To minimize the leakage from the containment and any subsequent release of fission products after an accident, it is necessary to reduce the pressure and temperature inside the containment. Also the capability to remove the additional energy produced by reactor decay heat must be provided, so that the containment design pressure is not exceeded. Since it is not permissible to cool the containment by means of once-through ventilation (due to the increased radioactive release to the environment) the containment ventilation systems and the Containment Spray System (CS) provide the required heat removal.

To further limit the release of radioactive iodine, the CS system includes a chemical additive (sodium hydroxide) to scrub any iodine from the containment atmosphere and keep it in solution in the containment sump water.

It is also necessary to control the buildup of hydrogen gas produced by the metal-water reactions in the core, evolution of dissolved hydrogen from the reactor coolant, and other sources to prevent reaching flammable or explosive levels. This is necessary to protect containment integrity and its support equipment. Post accident combustible gas control systems are capable of sampling and analyzing containment samples and reducing the hydrogen levels by use of thermal recombiners.

The design requirements of the containment also limit the amount of materials such as aluminum and zinc which will chemically react with hydroxyl ions in the reactor coolant to produce hydrogen in the containment in a post-accident environment.

5.4.2 Containment Ventilation Systems

The purposes of the containment ventilation systems are as follows:

1. To control the temperature and pressure of the containment during normal operations to maintain operability of the containment and associated equipment.
2. To provide localized area ventilation for equipment inside containment.
3. To provide cleanup of the containment atmosphere for limited personnel access while at power, and for continuous access while shutdown.

To amplify the purposes as previously stated, the containment ventilation system is designed to accomplish the following:

a. Limit the average containment temperature between 50 - 120 °F during normal operation.
b. Provide 70,000 CFM of air to the control rod drive mechanisms with a maximum inlet air temperature of 120 °F.
c. Supply air to maintain the Reactor Coolant Pump (RCP) air temperature below 120 °F.
d. Provide cooling air for the primary concrete shield and the enclosed nuclear instrumentation thimbles.
e. Provide air to cool the reactor vessel supports.
f. Control containment airborne fission product gases, halogens and particulates in order to allow containment access without exceeding the occupational exposure dose limits of 10 CFR Part 20.
g. Control the releases of fission product halogens, particulates, and noble gases during containment purge such that the requirements of 10 CFR Part 50, Appendix A, may be met for overall plant radioactivity releases.

Nine (9) systems, operating together, meet the diverse design requirements for containment ventilation. These systems are as follows:

1. Purge Supply System.
2. Purge Exhaust and Refueling Cavity Supply and Exhaust System.
3. Control Rod Drive Mechanism (CRDM) Cooling System.
4. Pressurizer Compartment and Incore Instrumentation Switching Room Cooling System.
5. RCP Cooling System.
6. Reactor Cavity Cooling System.
7. Containment Air Cooler System.
8. Unit Heater System.
9. Cleanup Recirculation Units.

5.4.2.1 Purge Supply System

The purge supply system (Figure 5.4-1) is designed to insure safe, continuous access to the containment within after a planned or unplanned reactor shutdown by reducing the airborne particulates of the containment atmosphere. The system performs no function with respect to reactor safety. Prior to activating the purge and exhaust systems, the particulate and radioactive gas activity levels inside the containment must be monitored and will be used as a guide for routing the release from the containment. A sample is taken and analyzed before purging begins. The containment is normally isolated from the environment during power operations, with purging at power limited by the plant's Technical Specifications.

The purge supply system consists of an outside air intake, an automatic roll filter, a bank of High Efficiency Particulate Air (HEPA) filters, two 100 percent supply fans arranged in parallel, backdraft dampers, an outboard air operated isolation valve, a containment penetration, an inboard motor operated isolation valve and associated duct work.

The duct work out to and including the containment outboard isolation valve is designed to Seismic Category I specifications. The isolation valves are quick closing and are capable of closing within five (5) seconds for the motor operated valves and within three (3) seconds for the air operated valves upon receipt of a Containment Ventilation Isolation Signal (CVIS).

The purge supply fans are 480 Vac, 3 phase, 125 horsepower vane axial fans, each is capable of providing 100 percent of the required 50,000 CFM of air. The fans are controlled from the main control room and are interlocked such that only one fan runs at a time. To start a fan, both isolation valves must be open and the other fan must be in off. A pressure switch that senses pressure in the common discharge ductwork will start the standby fan on low pressure if the running fan is lost. When starting a fan, the control switch for the redundant fan must be in Pull-To-Lock until the running fan has increased the duct pressure above the pressure switch setpoint. The supply fans also have undervoltage and overcurrent protection.

The automatic roll filter is an 80 percent efficient filter designed to reduce the particulate and dust in the supply air to serve as a prefilter for the HEPA filter. The filter drive motor is interlocked with the supply fans such that it will run when either fan is on and is deenergized by a filter runout interlock.

The inboard and outboard dampers are controlled from the main control room. With the control switch in the normal position (not in lockout) they will automatically close on either a CVIS, a containment high radiation signal (PERM), or a manual Containment Spray Actuation Signal (CSAS). Damper open and closed indication is sensed by limit switches and is provided at the control switch and also on both the Containment Isolation System (CIS) and CVIS status panels in the main control room.

5.4.2.2 Purge Exhaust and Refueling Cavity Supply and Exhaust System

The purge exhaust and refueling cavity supply and exhaust system (Figure 5.4-2) work in conjunction with the containment purge supply system to provide one and one-half (1 1/2) containment air changes per hour. The purge exhaust is operated in mode 5 and 6 when continuous containment occupancy is desired.

The purge exhaust system consists of an inboard motor operated isolation damper, a containment penetration, an outboard air operated isolation damper, an automatic roll filter, a bank of HEPA filters, two 100 percent exhaust fans arranged in parallel, backdraft dampers, and associated ductwork. These components meet the same requirements as noted for the purge supply system.

The purge exhaust system exhausts to the containment purge vent at the top of the containment building. Exhaust air is monitored for gaseous, particulate and iodine activity.

The refueling cavity supply consists of two (2) fans drawing air from the containment atmosphere and discharging horizontally across the refueling cavity. The refueling cavity exhaust consists of two (2) fans drawing air from the inlets at the surface of the refueling cavity and discharging to the purge exhaust system. The refueling cavity supply and exhaust system's design objective is to rapidly remove and exhaust water vapor and fission products escaping from the fuel pool surface, to reduce the burden in the containment atmosphere during refueling.

5.4.2.3 CRDM Cooling System

The CRDM cooling system (Figure 5.4-3) is designed to remove heat from the CRDMs and release it to the containment atmosphere. Air quantity and static pressure drop requirements are based on maintaining the CRDM temperatures at ≤300 °F with normal operation of two (2) of the four (4) fans and a containment air temperature of 120 °F. The system shall be in operation anytime the RCS temperature is ≥ 350 °F. The system draws a minimum of 70,000 CFM of air through the shroud enclosing the CRDMs an discharges it upward where it rises by convection to the containment air coolers. The four (4) fans are mounted on the CRDM missile shield. The system is Seismic Category II and is not connected to an emergency power supply.

5.4.2.4 Chill Water System

The chill water system (Figure 5.4-4) is not a safety related system, however, it is an important system that removes heat generated in the digital rod position indication and control cabinets, the pressurizer compartment, the incore instrumentation switch room, the reactor cavity, and the process sample system. The majority of the equipment is located in the containment where it is exposed to ambient temperatures that range from 90 °F to 110 °F. Any equipment cooled by chill water may overheat if flow is interrupted it is, therefore, necessary to run the chill water system as much as possible.

5.4.2.5 Pressurizer Compartment and Incore Instrumentation Switching Room Cooling System

The pressurizer compartment and incore instrumentation switching room cooling system (Figure 5.4-5) is designed to circulate containment air to these areas during normal operation and to supply 80 °F air when personnel must access these areas. The system consists of two independent systems, one for the pressurizer compartment and the other for the incore instrumentation switching room.

Each system consists of a dust filter, a chill water cooling coil, a supply fan, and distribution ductwork. The systems can cool their areas sufficiently for personnel entry by use of the fans and cooling coils, and are capable of maintaining suitable compartment temperature for normal equipment operation by use of the fans only. The cooling coils can be served by either of two chillers, each of which can provide 100 percent of the required design capacity. The system is designed as a Seismic Category II system.

5.4.2.6 Reactor Coolant Pump Cooling System

The RCP cooling system (Figure 5.4-6) is designed to distribute cooling air to each of the RCP motors. The system consists of four (4) independent subsystems, one for each RCP. Each subsystem consists of two (2) 100 percent capacity fans arranged in parallel, backdraft dampers, and associated ductwork The system is arranged so that the subsystem serving one RCP is entirely independent of the subsystems serving the other RCPs. The RCP cooling system is a Seismic Category II system.

5.4.2.7 Reactor Cavity Cooling System

The reactor cavity cooling system (Figure 5.4-7) is designed to circulate chilled air through the incore instrumentation tunnel and up through the cavity around the reactor vessel and its supports. The system is designed to handle the portion of the cooling load which occurs below the cavity seal. An upper exit air temperature limit of 110 °F is imposed on the system based upon the fact that this air subsequently enters the CRDM cooling system. The system is a Seismic Category II system.

5.4.2.8 Containment Air Cooler System

The containment air cooler system (Figure 5.4-8), when operating under normal conditions, and in conjunction with other normal containment ventilation systems, removes the heat losses from normally operating equipment and from radiation and convective transfer from the primary and secondary coolant systems.

The system provides the heat removal capacity to maintain containment temperature below 120 °F during normal plant operation. The system also has the capacity to significantly reduce the containment heat energy following a LOCA. The containment air cooler system is an Engineered Safety Features (ESF) system and is Seismic Category I.

The system consists of eight (8) individual air cooler units of equal capacity mounted above the containment spray header. Each unit contains a fan enclosed by an airtight roof and floor and surrounded on four sides by 12 cooling coils. The fans draw air horizontally across the cooling coils and discharge the cooled air downward into the containment. The cooling coils are supplied with cooling water from the Component Cooling Water System (CCW). The eight (8) air coolers are divided into two (2) groups of four (4) units. Each group of cooling units is designated as train A, and train B. Each of the four (4) train A cooling coils is supplied with cooling water from the train A CCW loop. Each of the four (4) train A cooler fans is supplied power from the train A 480 Vac ESF electrical bus. Air cooler fan and cooling coils for train B are similarly supplied. Physical separation and barriers are provided between all train A and train B components.

The containment air cooler system is designed to maintain containment air temperature below 120 °F during normal operation with six (6) of the eight (8) cooler units in operation when CCW is at design flow and temperature. The containment air cooler system will also remove heat energy from the containment atmosphere in the event of a LOCA in order to suppress any resultant increase in containment pressure and temperature. Additionally, the system is designed such that a single failure of any active component during the injection phase, or any active or passive failure during the recirculation phase, will not degrade the system's ability to meet the design objectives.

The air cooler fans are 480 Vac, three phase, 125 horsepower, downblast discharge, vane axial fans. Each fan has a design capacity of 100,000 CFM and is powered from the ESF electrical buses. The fan motors are designed to ensure required air and steam mixture flow is achieved under design basis event conditions. Under these conditions the fan motor output horsepower is increased because fan brake horsepower requirements vary with the density of the containment atmosphere.

The containment air cooler fans are normally controlled from the main control room. The control switches have STOP, NORMAL, and START positions with PULL-TO-LOCK and spring return to NORMAL features. In NORMAL, the air coolers can be automatically started by the DBA load sequencer.

During normal operation the CCW system supplies both containment air cooler trains. The CCW supply line has two (2) motor operated valves which are normally closed with an orificed bypass line which supplies 1950 gpm of CCW to each train. The air cooler fans are started as necessary to maintain containment temperature between 50 and 120 °F. Not more than three (3) air coolers in each train are run simultaneously except for periodic testing. Normal air cooler operation has six (6) of the eight (8) coolers in operation. In modes 1 - 4, at least three (3) of the coolers in each train shall be running.

Humidity in the air will condense on the coolers. The condensation from the coolers is collected in a drip pan below each cooler. The drip pans are connected to a common collection header and directed to a condensate collection pot. When the level in the pot reaches a setpoint, a motor operated valve opens and allows the pot to drain to the containment sump. The number of times that the motor operated valve opens is recorded in the control room. Condensate pot drain cycles are proportional to the condensation rate. The condensation rate is proportional to humidity and CCW temperature. Humidity is proportional to the leak rate of liquid systems inside the containment.

A Safety Injection Signal (SI) causes startup of any standby CCW train and the separation of the two CCW trains. The motor operated valves in the containment air cooler supplies open and provide a minimum of 6000 gpm flow to each cooler train. The DBA load sequencer automatically starts any air cooler fans that are in NORMAL.

5.3.2.9 Unit Heater System

The unit heater system consists of ten unit heaters located throughout the containment building. The unit heaters are designed to provide heating to allow for personnel comfort during periods of personnel access. The electrical heating coils and blower units are locally controlled and have a variable temperature control.

5.3.2.10 Cleanup Recirculating Units

During normal operation two (2) Seismic Category II recirculating filter units are available for intermittent or continuous operation to control the buildup of airborne halogens and particulates which result from small RCS leaks within the containment. The cleanup filters (in conjunction with the containment purge system) have two (2) objectives. The first is to maintain airborne fission product levels below the 10 CFR Part 20 limits for occupational exposures to allow safe access to the containment. The second is to reduce fission product releases to the environment to levels as low as reasonably achievable when containment purging is required. The cleanup recirculation system performs no function with respect to reactor safety.

The cleanup recirculation system (Figure 5.4-9) consists of two (2) separate units. Each unit draws 4000 CFM if containment air through a prefilter, a HEPA filter, and a carbon absorber. With both units in operation, approximately one (1) containment air volume will be recirculated every four (4) hours.

5.4.3 Containment Hydrogen Control

Three (3) systems are designed to control hydrogen in the containment building. The systems are the hydrogen control system, the hydrogen mixing system and the hydrogen vent

5.7 AUXILIARY FEEDWATER SYSTEM

Learning Objectives:

1. State the purposes of the Auxiliary Feedwater (AFW) system.
2. List all suction sources for the AFW pumps and under what conditions each is used.
3. List the five plant conditions that will result in an automatic start of the AFW system.
4. Explain how decay heat is removed following a plant trip and loss of offsite power.
5. Explain how a minimum volume of water in the condensate storage tank is reserved for the AFW system.

5.7.1 Introduction

The purposes of the AFW system are as follows:

1. Provide feedwater to the steam generators to maintain a heat sink for the following conditions.
   a. Loss of main feedwater (MFW).
   b. Unit trip and loss of offsite power.
   c. Small break loss of coolant accident.
2. Provide a source of feedwater to the steam generators during plant startup and shutdown.

The AFW system supplies, in the event of a loss of the main feedwater, sufficient feedwater to the steam generators to remove primary system stored heat and residual core energy (decay heat). AFW must also be available under accident conditions, such as a small break loss of coolant accident, so the plant can be brought to a safe shutdown condition.

The AFW system is designed to automatically start and supply sufficient feedwater to prevent the relief of primary coolant through the pressurizer safety valves. The AFW system has an adequate suction source and flow capacity to maintain the reactor at hot standby for a period of time and then cool the Reactor Coolant System (RCS) to a temperature at which the Residual Heat Removal System (RHR) may be placed in operation.

5.7.2 System Description

The AFW system as shown in Figure 5.7-1, has two electric-motor-driven pumps and one turbine-driven pump. Each of the electric driven pumps supplies two different steam generators, the turbine driven pump supplies all four steam generators. All three pumps automatically deliver rated flow within 1 minute upon receipt of an automatic start signal.

The preferred source of water for all auxiliary feedwater pumps is the Condensate Storage Tank (CST) which is required by the plants Technical Specifications to contain a minimum amount of water to be used by the AFW system. An additional unlimited backup water supply, Essential Service Water (ESW), is supplied to the AFW system. A separate train of ESW feeds each electric driven pump, (Train A of ESW feeds the A AFW pump) while the turbine driven pump can receive backup water from either train of ESW.

To protect the AFW pumps from a loss of suction, the ESW supply valves are automatically (or remote-manually) opened if the suction pressure is low on two-out-of-three pressure detectors, and the AFW pump is running.

Since the ESW system supplies poor quality water, it is not used except in emergencies when the normal condensate supply is unavailable.

The AFW system is designed to deliver 40 to 120°F water for pressures ranging from the RHR system operating pressure (equivalent to approximately 110 psig in the steam generators) to the highest set point of the steam generator safety valves (1234 psig).

The AFW system piping is designed for pressures up to approximately 1650 psig where necessary. Separate Engineered Safety Features (ESF) quality electrical power subsystems and control air subsystems serve each AFW pump and its associated valves.

In addition to using high quality components and materials, the AFW system provides complete redundancy in pump capacity and water supply for all cases for which the system is required. Under all credible accident conditions each steam generator, not affected by the accident, will be supplied with its required feedwater. Only two steam generators are required to be operable for any credible accident condition.

Redundant electrical power and air supplies assure reliable system initiation and operation. The electric-motor-driven pumps are powered from vital ac distribution sources, while the turbine-driven pump takes steam from either of two main steam lines, up stream of the main steam isolation valves (MSIVs).

5.7.3 Component Descriptions

5.7.3.1 Motor Driven Auxiliary Feedwater Pumps

The motor driven pumps are multi-stage horizontal centrifugal pumps, each of which supplies 440 gpm at a discharge pressure of about 1300 psig. The motor driven pump design data is shown in Table 5.7-1.

Power to the motor driven AFW pumps is supplied from the 4.16 kVac Class IE vital distribution boards. Local switches permit local operation of the pumps. The switches in the control room have three positions: Run, Stop, and Pull to Lock. The Pull to Lock feature prevents the pumps from starting, even if an automatic start signal were present.

Table 5.7-1
Auxiliary Feedwater System
Design Data

Total number of pumps per unit	3
Motor driven	2
Turbine driven	1
Design flow rate, gpm	
Motor driven, each	440
Turbine driven	880
System design pressure, psig	1650
Design feedwater temperature, ° F	40-120
Design discharge head, psig	
Motor driven	1300
Turbine driven	1200

The following five conditions will automatically start both motor driven feed pumps:

1. Low-low steam generator level in any single steam generator.
2. Loss of one main feed pump (MFP) if power is greater than 80 percent.
3. Loss of both MFPs at any power level.
4. ESF actuation signal.
5. Loss of power to the Class IE power distribution system.

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

LIST OF FIGURES

3. for remote operation, the synchronizing switch must be on. For local operation, the EDG output ACB must be tripped.

An ESF bus feeder ACB trips automatically if any one of the following occurs:

1. a bus lockout signal is generated,
2. a unit substation transformer lockout signal is generated,
3. a bus undervoltage relay actuates and the associated EDG automatically starts and attains normal speed and voltage, or
4. a bus voltage greater than 2.56 kv but less than 3.85 kv is maintained for greater than 55 seconds

A bus lockout is caused by either a phase overcurrent or a ground overcurrent on the bus feeder. This condition energizes the lockout relay and trips the ESF bus feeder ACB and removes a permissive for closing the EDG output ACB.

An ESF bus undervoltage condition energizes the undervoltage auxiliary relays. The undervoltage auxiliary relay will cause the following:

1. a trip of the bus feeder ACB,
2. Trips of all 4.16-kv load ACBs except those which supply load centers,
3. a start signal for the associated EDG,
4. a permissive to close the EDG ACB,
5. delaying the DBA or shutdown sequencer from operating until voltage is restored to the bus,
6. an auxiliary feed pump start permissive, and
7. energizing of the undervoltage relays, which trip all containment air coolers and non-essential 480-v loads.

Two levels of undervoltage protection are provided. Primary protection is provided against an undervoltage of less than 2560 volts for greater than one second. The one second time delay is selected because motor damage could be sustained if operation were to continue at this low voltage for greater than 1.1 seconds.

Secondary protection, commonly referred to as degraded grid protection, is provided against an undervoltage of less than 3850 volts. "Degraded grid" is a term describing a low voltage condition affecting an ESF bus which results in a voltage on the bus that if sustained longer than 60 seconds could result in motor insulation damage due to the higher than normal currents. If a safety injection signal (SIS) is present, the normal feeder is closed, and voltage drops to less than 3850 volts for more than 4 seconds, the undervoltage relay is energized. If there is not an SIS present, then the undervoltage condition must continue an additional 51 seconds (a total of 55 seconds) before the undervoltage relay energizes.

6.3.2.6 DBA and Shutdown Sequencers

Upon initiation of a diesel generator start signal and closure of the EDG ACB, certain small loads supplied from the ESF motor control centers are energized immediately since they are not stripped on undervoltage. To allow the EDGs to start unloaded, the undervoltage scheme will strip all large motor loads (including the containment air coolers) and non-ESF loads off the 4.16-kv bus and connected 480-volt load centers. Depending on the plant conditions at the time of the initiating event, either of two sequencers will begin loading the bus either to safely shut down the plant or to meet emergency needs in response to a safety injection signal.

Each sequencer consists of Agastat timers which are simultaneously energized and which perform their functions in a timed sequence. The DBA sequencer consists of 10 Agastat timers. The shutdown sequencer consists of four timers. The sequence and timing for energizing loads in accordance with the DBA sequencer are shown in the following table:

Sequence	Load	Time (sec)
1.	CCP and ESF Switch-gear room coolers	2.0
2.	Safety injection pump	6.5
3.*	Containment spray pump	11.0
4.	RHR pump	15.5
5.	CCW pump	20.0
6.	SW pump	24.5
7.	Containment air coolers	29.0
8.*	Containment spray pump	40.0

* The containment spray pump has two separate start signals. The first start signal at 11 seconds will start the pump only if there is also a simultaneous Hi-Hi containment pressure signal. If the pump starts, it will continue to run. If there is not a simultaneous Hi-Hi containment pressure signal with the 11-second start signal, the pump will not be enabled to start until the second start signal at 40 seconds. The 40-second start signal locks in, after which the pump will start whenever a Hi-Hi containment pressure signal is received. This feature prevents spurious starting of the containment spray pump during the interval from 11 to 40 seconds when other loads are being started on the diesel generator.

The sequence and timing for energizing loads in accordance with the shutdown sequencer are shown in the following table:

Sequence	Load	Time (sec)
1.	CCP and ESF Switch-gear room coolers	2.0
2.	CCW pump	6.5
3.	SW pump	11.0

(Note that auxiliary feedwater [AFW] pumps do not appear on the lists of equipment powered by ESF buses or as equipment energized by the DBA and shutdown sequencers. The AFW system modeled by the Westinghouse simulator [described in Chapter 5.8] has no motor-driven pumps which have to be loaded onto ESF buses, so the steam-driven and diesel-driven pumps of that system are started directly by an SIS or by an ESF bus undervoltage condition. For a plant with a more typical AFW system like that described in Chapter 5.7, each motor-driven pump would be supplied by a separate ESF bus, and each motor-driven pump would be energized [probably late in the sequence] by both sequencers associated with its train.)

In general each Agastat timer serves a dual function: it starts the next load in the starting sequence and removes the start demand from the previous load in the starting sequence. As an example, with the DBA sequencer, the centrifugal charging pump is started at 2 seconds, and the start circuit is "opened" at 6.5 seconds when the safety injection pump is started. This feature prevents the simultaneous starting of more than one motor on the EDG, which could damage the generator or actuate protection. Exceptions to this scheme are the start signals for the containment air coolers and service water pumps. Another exception to this scheme is the "lock-in" signal for the containment spray pump. When the timer energizes it bypasses the first start circuit and does not have another relay to reopen its circuit. The DBA sequencer must be reset (SIS reset) to remove the start signal from the pump circuit.

Each DBA sequencer requires only the initiation of a safety injection signal and the availability of voltage on the associated 4.16-kv bus to energize and begin its sequence. Therefore, it does not absolutely require the start of the EDG or the initiation of the undervoltage scheme to function. The shutdown sequencer is designed to function after a loss of offsite power to enable a safe shutdown of the plant. In order for it to energize, the EDG must be at rated speed and voltage, the EDG ACB must be closed, and power must be restored to the 4.16-kv bus. If a safety injection signal occurs simultaneously with the loss of offsite power, the shutdown sequencer will not energize, but as soon as power is restored to the bus the DBA sequencer will start. It is important to note that even though the sequencers will start specific loads automatically, there is nothing to prevent the operator from starting any load at any time. Furthermore, once a load is sequenced on, there are no interlocks in the load circuitry to prevent opening its ACB, whether inadvertent, intentional, or automatic. (Only the last containment spray pump to start is equipped with a "lock-in" signal. This relay prevents tripping except when the switch is placed in the pull-to-lock position and is in the circuit until the SIS is reset.) However, it should be noted that the containment spray pumps will operate only when a Hi-Hi containment pressure of 30 psig is reached.

6.3.2.7 Non-ESF Switchgear A5 and A6

The non-ESF buses provide power to vital loads necessary for plant operation but not necessarily required for reactor shutdown in the event of a design basis accident. The A5 and A6 switchgear and the ACB controls and operations are identical to those of the ESF switchgear discussed earlier.

Bus A5 supplies the following loads:

1. heater drain pump A
2. cooling tower makeup pump A
3. pressurizer heater load center
4. several load centers
5. startup auxiliary feed pump
6. A5/A6 bus tie ACB.

Bus A6 supplies the following loads:

1. heater drain pump B
2. cooling tower makeup pump B
3. pressurizer heater load center
4. several load centers
5. a motor control center.

All load ACBs on buses A5 and A6 have the same protection devices as those discussed in the ESF bus description. That is, the motor ACBs are equipped with ground and overcurrent trips and thermal overload alarm protection. All other loads have only the ground and overcurrent trips. On an undervoltage condition on a non-ESF bus, all load ACBs will trip, including the load center ACBs. Undervoltage protection for the non-ESF buses is more simplified than that for the ESF buses and consists of two undervoltage relays per bus. Upon sensing an undervoltage of 2.5 kv, the undervoltage relays energize a one-second timer (to allow for transient voltage dips); the timer energizes a relay which completely strips the bus. For this reason all loads on buses A5 and A6 will require restarting/re-energizing following a sustained loss of voltage for greater than 1 second.

6.3.2.8 Bus A5/A6 Tie ACB

Buses A5 and A6 can be connected through an ACB. Although rated at 1200 amp, this ACB is limited to 800 amp due to metering limitations. This rating may become limiting during abnormal electric lineups in which one unit substation transformer is supplying all buses.

To close the A5/A6 tie ACB, the following conditions must be satisfied:

1. the synchronizing switch must be on,
2. bus A5 and A6 lockout relays must be reset, and
3. either bus H1 or H2 must be energized.

It is important to note that regardless of whether the ACB is operated remotely or locally, the synchronizing switch must be on. For other ACBs discussed in previous sections of this chapter, this prerequisite applies only to remote closing of an ACB. With regard to the A5/A6 tie ACB, even if one of the buses is de-energize, the synchronizing switch must still be on.

The A5/A6 tie ACB trips automatically if any one of the following occurs:

1. a bus lockout signal,
2. low voltage on both 12.47-kv buses, or
3. phase or ground overcurrent protection is actuated.

The A5 and A6 bus feeder ACBs are operated locally or from the control room. To close a non-ESF bus feeder ACB:

1. the synchronizing switch must be on for both local and remote operation,
2. the unit substation transformer lockout relay must be reset, and
3. the bus lockout relay must be reset.

A non-ESF bus feeder ACB trips automatically if either of the following occurs:

1. a bus lockout signal, or
2. a unit substation transformer lockout signal.

6.3.3 Summary

The 4.16-kv electrical system consists of four buses. Two of these buses are classified as ESF buses which supply power to equipment that is vital for the safe shutdown of the reactor plant. The two non-ESF buses, supply power to equipment that is vital for plant operation but not needed to achieve a safe shutdown condition.

6.4 480-vac Electrical System

The 480-vac electrical system is the most extensive electrical system in the plant, supplying a majority of plant electrical loads. This system supplies power to both ESF and non-ESF load groups. The ESF portion is required to enable a safe shutdown of the reactor in the event of a plant accident. The ESF load centers and motor control centers supply power to two physically and electrically independent load groups, each of which is capable of supplying the necessary auxiliaries to safely shut down the reactor. In addition to the normal and auxiliary power sources, the 4.16-kv ESF safety trains, and in turn the 480-vac ESF loads, are supplied with standby diesel generator power (to permit a safe reactor shutdown and long-term cooling capability for all design conditions.)

6.4.1 Detailed Description

The 480-vac electrical system is designed to provide sufficient power for both the ESF and non- ESF loads from load centers and motor control centers. The motor control centers supply small motor loads, station lighting, battery chargers, and 208/120-vac instrument buses through transformers.

The 480-vac electrical system is divided into three separate categories:

1. the 480-vac ESF electrical system,
2. the 480-vac non-ESF electrical system, and
3. the 480-vac heating and ventilating electrical system.

The ESF portion of the system (Figure 6-5) is powered by the 4.16-kv electrical system buses A1 and A2 directly through four 4.16-kv/480-v step-down transformers. Each train of the 480-vac electrical system powers 100% redundant vital loads and is in turn powered from a separate 4.16-kv bus. In other words, safety systems have identical components powered from independent and electrically separated power supplies, such that in the unlikely event that one of the safety buses fails, the other bus is capable of completely performing its intended safety function.

The non-ESF portion of the 480-vac system is powered from 4.16-kv electrical system buses A5 and A6 directly through 10 4.16-kv/480-v step-down transformers. Both the heating and ventilating portion and the non-ESF portion of the system are divided to permit the maximum operability and reliability possible.

The 480-vac heating and ventilating electrical system is supplied from 12.47-kv electrical system buses H1 and H2 directly through eight 12.47-kv/480-v step-down transformers. This portion of the 480-vac system is divided such that approximately one half of the load groups are supplied from bus H1 and the remaining load groups are supplied from bus H2.

All of the 480-vac systems consist of the following major components:

1. Load centers (LCs) - the large distribution switchgear which contains metal-enclosed, drawout-type air circuit breakers. The LCs supply motor control centers and motors of greater than 100 hp.
2. Motor control centers (MCCs) - distribution points which supply the majority of in-plant loads. MCCs contain molded- case circuit breakers, motor controllers, and transformers.
3. Circuit breakers - interrupting devices utilized to connect and disconnect LCs, MCCs, and individual loads from the particular power supply.
4. Transformers - devices utilized to change an ac voltages and currents. A transformer can be either a stepup (voltage increase) or step-down (voltage decrease) transformer. The current varies inversely with voltage. The current is also dependent on the load on the transformer.

6.4.2 Component Descriptions

6.4.2.1 Transformers

The majority of transformers utilized throughout the 480-vac systems are of the indoor, dry, air-cooled type. Three transformers installed outdoors are sealed and filled with octafluorocyclobutane (C_4F_8), an inert gas. The heating and ventilating electrical system transformers are rated for 12.47 kv and the ESF and non-ESF electrical system transformers are rated for 4.16 kv. Most of the secondaries of the transformers are connected in a grounded "Y" configuration yielding an output of 480 vac. The delta-wye configuration used on most transformers enhances fault isolation. This configuration acts as a filter such that instabilities on the high voltage side of a transformer are not transferred to the low voltage side of that transformer. The transformers which power the pressurizer heaters are connected in delta-delta configurations to enable single-phase 480-vac power to be taken from the transformer secondaries, which is required to operate the heaters. All transformers utilized in the 480-vac system are rated from 500 kva to 1000 kva.

6.4.2.2 Circuit Breakers

Two types of circuit breakers are utilized throughout the 480-vac distribution system, air circuit breakers and molded-case breakers. Air circuit breakers are large metal-enclosed, drawout-type circuit breakers located in the load centers. Smaller molded-case breakers are utilized as the 480-vac MCC load feeders. These breakers have a lower current rating than that of the air circuit breakers. They are not provided with remote operating capability since they normally do not provide control functions for their associated load.

6.4.3 Summary

The 480-vac electrical system supplies a majority of plant electrical loads. This system supplies power to both ESF and non-ESF load groups. The ESF portion is required to enable a safe shutdown of the reactor in the event of a plant accident.

6.5 120-vac Electrical System

The 120-vac electrical system is designed to provide reliable power for control and instrumentation. The 120-vac electrical system is composed of the following subsystems:

1. preferred system
2. nonpreferred system.

The preferred system is safety related. It provides control and instrumentation power to equipment that is required for the safe shutdown of the reactor.

The nonpreferred system, which is also called the 208/120-v instrument system, is not safety related. It provides power to equipment that is not required for the safe shutdown of the reactor.

6.5.1 Preferred System

The preferred system is composed of two physically separate, electrically independent, redundant trains. Each train consists of two preferred instrument buses and two inverters (Figure 6-6).

Each train is made up of two channels, which are color coded because of their safety functions. Train A consists of channels I (red) and III (blue), and train B consists of channels II (white) and IV (yellow).

The purpose of the preferred system is to supply reliable, continuous Class 1E electrical power to the engineered safety feature (ESF) equipment, the four reactor protection system (RPS) channels (I, II, III, and IV), and essential plant instrumentation and control equipment required for plant startup, operation, and shutdown. Note that the system provides this power under all conditions, including the complete loss of offsite and onsite power.

The preferred system satisfies the following design criteria:

1. seismic qualification
2. quality assurance
3. redundancy/diversity
4. environmental qualification
5. fire protection
6. environmental protection.

The seismic criteria are satisfied because the system is designed to withstand the effects of earthquakes without the loss of the ability to perform its safety functions. Since the preferred system is designed to remain functional in the event of a safe shutdown earthquake, it is designated safety related and Seismic Category I (SCI).

The quality assurance criteria are satisfied because the system is designed, fabricated, created, and tested to quality standards commensurate with the importance of the safety functions to be performed.

The redundancy/diversity criteria are satisfied because the system has sufficient independence, redundancy, and testability to perform its safety function assuming a single failure. The preferred system satisfies the following specific redundancy/diversity requirements:

1. The system is an uninterruptable power system with diverse onsite power supplies as

input sources. The input sources are of the same ESF train (A or B) as the inverters they supply,

2. The system has physically separate and independent trains to support the two trains of ESF loads (A and B) and the four RPS channels (I, II, III, and IV),
3. Each train is redundant with no cross connection between trains so that a failure in one train does not affect the other, and
4. Each train supplies electrical power at a sufficient capacity for plant startup, operation, or shutdown with a total loss of main ac power, and assuming the worst-case accident loading.

The environmental qualification criteria are satisfied because the system is designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss of coolant accidents.

The fire protection criteria are satisfied because the system is designed and located to minimize the probability and effects of fires and explosions.

The environmental protection criteria are satisfied because the system is designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without the loss of the ability to perform its safety functions, and because the system is appropriately protected against dynamic effects, including missiles, pipe whips, and discharging fluids.

Figure 6-7 shows that each inverter has two power supplies, each of which is ultimately powered from a 4.16-kv ESF bus. The normal power supply is an underground 125-vdc bus. The alternate power supply is a 480-vac motor control center. If the normal power supply should fail, the inverter will automatically shift to its alternate power supply to prevent an interruption of power to the associated preferred instrument bus.

Each preferred instrument bus also has two power supplies, but only one of these is ultimately powered from an ESF bus. An inverter is the normal (Class 1E) power supply for each preferred instrument bus. A nonpreferred instrument bus is the alternate (non-Class 1E) power supply for each preferred instrument bus. Figure 6-7 shows that the alternate power supplies completely bypass the inverters and their two sources of Class 1E power. Note that the only time a preferred instrument bus is powered from its alternate power supply is when its normal power supply must be removed from service for maintenance or repair.

Unlike the power supplies for the inverters, the power supplies for the preferred instrument buses are not equipped with an automatic transfer feature; therefore, when an inverter fails or needs maintenance, the associated preferred instrument bus power supply must be manually transferred to its alternate source.

Consider a preferred instrument bus. Normally, an inverter supplies power to the bus. When the inverter is not available, the bus can be powered from a nonpreferred bus. The main feeder breakers to the preferred bus are mechanically interlocked such that if one is closed, the other opens. Since they are "break-before-make" connections, both breakers cannot be closed simultaneously; however, both breakers can be opened simultaneously to de-energize the bus. This interlock prevents the Class 1E and the non-Class 1E power supplies from being electrically paralleled.

The major loads on train A of the preferred electrical system include ESF train A equipment and RPS channels I and III. The major loads on train B of the system include ESF train B equipment and RPS channels II and IV. Since the ESF loads and circuits are divided into two completely redundant groups which are electrically independent and physically separated, only one preferred instrument train is needed to achieve and maintain a safe shutdown condition.

6.5.1.1 Inverters

Although the component shown in Figure 6-7 is commonly referred to as an "inverter," it is not a true inverter. Instead, it is an uninterruptable power supply (UPS) because it provides the preferred instrument buses with uninterruptable power from two Class 1E sources. However, since these components are frequently called "inverters," that is what they will be called in this system description.

The true inverters are the components within the UPSs that actually convert 125-vdc power into 120-vac power. These components will be called "static inverters" in order to distinguish them from the UPSs, or "inverters."

Figure 6-7 shows the four basic components installed in each inverter cabinet. These components are:

1. a dc-to-ac solid-state static inverter,
2. a solid-state static switch,
3. a 480/120 v transformer, and
4. a manual bypass switch.

The function of the static inverter is to convert the 125-vdc input into a single-phase, 120-vac, 60-hz output. The static inverter provides the normal source of preferred instrument power. The function of the static switch is to automatically transfer the selected source of preferred instrument power from the static inverter to the transformer if the static inverter fails. The function of the transformer is to step down a single phase of the 480-vac input to a 120-vac, 60-hz output. The transformer provides the alternate source of preferred instrument power. The function of the manual bypass switch is to allow the static inverter and static switch to be manually bypassed for maintenance or repairs.

During normal operation of the preferred system, each static inverter converts the 125-vdc input power to a 120-vac output power, which is fed through the static switch and the manual bypass switch to the associated preferred instrument bus.

If the alternate power source is energized, the static switch of an inverter will automatically transfer to the alternate power source when any of the following static inverter faults is sensed:

1. low input voltage
2. low output voltage
3. high output voltage
4. high output current
5. low control logic voltage.

(Note:The static switch is not "normal seeking"; therefore, if the static switch automatically transfers the load to the alternate source and the normal source is later restored, it will not automatically transfer the load back to the normal source. This will have to be done manually.)

6.5.2 Nonpreferred System

The nonpreferred system consists of four buses which are powered from the 480-vac system through three bus transformers as shown in Figure 6-6. The nonpreferred system supplies reliable power to various indication and control circuits that are necessary for the proper operation of the plant, but are not required to be operable in order to achieve a safe reactor shutdown.

The nonpreferred buses are powered from 480-vac ESF motor control centers (MCCs). The supply breakers from the MCCs are mechanically interlocked via input bus transfer switches to prevent any pair of supply breakers from being closed at the same time. This feature ensures that the ESF MCCs are not electrically paralleled through the nonpreferred instrument buses. Power from the MCCs is applied to regulating transformers, each of which provides three single-phase outputs of 120-vac power for system distribution.

Most of the loads on the nonpreferred instrument buses are indicating and control panels and various control valves. As shown in Figure 6-6, bus Y01 can supply the train A preferred instrument buses, although that is not the normal lineup. Similarly, bus Y02 can supply the train B preferred instrument buses. In addition, buses Y01 and Y02 power the digital rod position indication cabinet through a transfer switch which ensures that the cabinet is powered from only one source at a time (normally Y01).

6.5.3 Summary

The 120-vac electrical system provides reliable power for control and instrumentation. The 120-vac electrical system is composed of the preferred system and the nonpreferred system. The preferred system is safety related and provides control and instrumentation power to equipment that is required for the safe shutdown of the reactor. The nonpreferred system is not safety related and provides power to equipment that is not required for the safe shutdown of the reactor.

6.6 125-vdc Electrical System

The purpose of the 125-vdc electrical system is to supply reliable, continuous Class 1E electrical power to engineered safety feature (ESF) equipment and non-safety-related equipment required for startup, normal operation, and safe shutdown of the plant. The 125-vdc system provides this power for a specified time under all plant conditions, including the complete loss of offsite and onsite ac power sources.

6.6.1 System Description

The 125-vdc electrical system is composed of two physically separate, electrically independent, redundant trains. Figure 6-8 shows the arrangements of both trains. Each train contains a large lead-acid battery. The batteries are continuously connected to the dc distribution system and are maintained in a fully charged condition by their respective battery chargers during normal plant operations. The batteries have a passive role in the system during normal operations. When an abnormal condition results in a failure of the battery charger to power all dc loads, the associated battery is called upon to provide the necessary power, thereby ensuring continuity of operation. The batteries may only be needed during the short period required for starting the emergency diesel generators (EDGs), or they may be called upon to supply power for an extended period of time in the event of a loss of all ac power. In either case, it is absolutely essential that the batteries function properly if the plant safety systems are to operate as required.

Each train provides power for a redundant ESF load group, and is arranged so that the battery or any one charger can independently supply the buses in that train. Normally, one battery charger in each train rectifies 480-vac power to 125-vdc power to supply the system loads and to maintain the battery in a fully charged condition. The battery in each train will supply the system loads if the in-service battery charger fails or if a complete loss of offsite and onsite ac power occurs.

The 125-vdc system satisfies the following design criteria:

1. seismic qualification
2. quality assurance
3. redundancy/diversity
4. environmental qualification
5. fire protection
6. environmental protection.

The seismic qualification criteria are satisfied because the system is designed to withstand the effects of earthquakes without the loss of the ability to perform its safety functions. Since the 125-vdc system is designed to remain functional in the event of a safe shutdown earthquake, it is designated safety related and Seismic Category I.

The quality assurance criteria are satisfied because the system is designed, fabricated, created, and tested to quality standards commensurate with the importance of the safety functions to be performed.

The redundancy/diversity criteria are satisfied because the system has sufficient independence, redundancy, and testability to perform its safety functions assuming a single failure. The 125-vdc system satisfies the following specific redundancy/diversity requirements:

1. The system is an ungrounded dc system for safety and greater reliability,
2. The system has physically separate and independent trains to support the two trains of ESF loads (A and B),
3. Each train is redundant, with no cross-connections, so that the failure of one train does not affect the other, and
4. Each train supplies dc electrical power at a sufficient capacity for normal plant startup, operation, or shutdown and during a total loss of ac power if there is a worst-case accident loading.

The environmental qualification criteria are satisfied because the system is designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss of coolant accidents.

The fire protection criteria are satisfied because the system is designed and located to minimize the probability and effects of fires and explosions. Fire detection and suppression systems minimize the adverse effects of fire.

The environmental protection criteria are satisfied because the system is designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without the loss of the ability to perform its safety functions, and because the system is appropriately protected against dynamic effects, including missiles, pipe whips, and discharging fluids.

Figure 6-8 shows that each battery charger is powered from a different 480-vac ESF Motor Control Center (MCC). Normally, each train is aligned such that the dc buses are cross-connected through the battery breakers with the bus tie breaker open. This arrangement improves reliability during fault conditions because the bus tie breaker is a non-tripping breaker. Since the battery chargers are not designed with load-sharing capabilities, only one battery charger is in operation to supply the bus loads and maintain the battery in a fully charged condition. Figure 6-8 shows that the major loads on each train include two inverters, two dc distribution panels, and emergency dc lighting (which is usually selected to train B).

The dc distribution panels supply power to the following types of loads: annunciators, indicating lights, solenoid valves, control relays, small dc motors, switchgear (close and tripping power for all 12.47-kv, 4.16-kv, and some 480- v breakers), reactor trip and trip bypass breakers (close, trip, and indication power), and the EDGs (field flash, air start solenoid, control circuit, and fuel pump power).

6.6.2 Component Descriptions

6.6.2.1 Battery Chargers

The battery chargers are the normal power supplies for the dc buses. The basic components installed in each battery charger cabinet are:

1. an input power breaker,
2. a 480/120-v transformer,
3. a solid-state rectifier,
4. an output power breaker, and
5. a charger failure relay.

The function of the input power breaker is to supply the transformer with power from the 480-vac ESF MCC. The function of the transformer is to step down the 480-vac input from the MCC to a 120-vac output. The transformer also provides physical separation between the 480-vac system and the 125-vdc system. The function of the solid-state rectifier is to convert the 120-vac output from the transformer into a smooth, nominal 125-vdc output. The function of the output power breaker is to supply the output from the rectifier to the 125-vdc ESF bus. The function of the charger failure relay is to detect a loss of charger output due to a failure in the charger's ac power input or dc power output. The charger failure relays supply a common trouble alarm for each train. The alarm associated with the charger failure relays is delayed approximately 45 seconds by the alarm circuitry in order to prevent normal fluctuations in the charger output from causing a false alarm.

The battery charger is provided with a fail-safe filtering circuit across the output to limit any transient change in dc voltage to $\pm 2\%$ of the rated voltage in the event that the battery is disconnected from the charger. The charger is designed to prevent the battery from discharging back into any internal charger load in the event of an ac power supply failure or a charger failure.

The maximum post-accident steady-state load with ac power available is only 171 amp per charger (assuming only one charger per train is in service). Since each charger is rated for 200 amp, a single charger per train would be capable of carrying the required post-accident loads while recharging the battery in that train.

6.6.2.2 Batteries

The batteries serve as backup dc power supplies for the 125-vdc buses. If the operating battery charger in a train should fail, the associated battery will automatically supply power to the dc buses until the standby battery charger can be placed in service. In the event of a loss of a station blackout, the batteries will automatically supply power to the dc buses until ac power is restored (e.g., by automatic startup of the EDGs) or for a specified time interval which depends on the loads being supplied.

The proper battery size (i.e., battery capacity) for the plant is determined by the amount of starting and running current each load draws and the length of time each load needs to be supplied from the batteries during an accident. Note that emergency lighting is selected to train B. Also, note that the train A battery is required to be operable for two hours, but the train B battery is required to be operable for only 30 minutes. The battery duty cycles, or accident load profiles, are created from the list of design loads by plotting the total current drawn by those loads versus time.

Each battery is located in a separate room.

The battery room exhaust system continuously operates to ventilate the battery rooms to reduce any hydrogen accumulation (especially during charging operations), and exhausts it to the atmosphere. A loss of ventilation will not result in hazardous hydrogen levels until approximately 15 days later. In addition, the loss of ventilation to either battery room is annunciated in the control room. Each room has a space heater to maintain the air temperature between 70°F and 80°F. A low air temperature in either battery room is also annunciated in the control room. The combined effects of ventilation and the battery room space heaters ensure that the maximum temperature spread for all connected cells does not exceed 5°F. Operation with high temperature gradients between cells contributes to nonuniform charging and premature aging of cells.

Each battery consists of 60 cells which are series connected to achieve a nominal terminal voltage of 125 v. Each lead-acid battery cell consists of a group of positive and negative electrodes, or plates, connected together and encased in a vented, transparent container.

6.6.3 Summary

The 125-vdc electrical system supplies reliable, continuous Class 1E electrical power to ESF equipment and non-ESF equipment required for startup, normal operation, and safe shutdown of the plant. The 125-vdc system provides this power for a specified time under all plant conditions, including the complete loss of offsite and onsite ac power sources.

6.7 Main Generator

The main generator produces electrical power and transmits that power to the offsite distribution system. It also supplies power for normal operation of the nuclear generating unit through the unit auxiliary transformer.

Power is taken from the main generator through a high voltage bushing assembly and transmitted through the isolated phase bus to the main transformer. The voltage is stepped up from 22 kv to 230 kv by the main transformer for delivery to the high voltage overhead transmission system. Figure 6-9 provides a basic illustration of the system.

6.7.1 Detailed Description

The main generator, located in the turbine building, is driven at 1800 rpm by the main turbine and converts the mechanical energy of the turbine into 3-phase, 22-kv, 60-hz electrical power at a 1,280,000-kva rating. The unit is a four-pole, wye-connected machine with a rated power factor of .95. Its construction consists of the casing, the stator core, the rotor, the inner and outer end shields, and bearings.

6.7.1.1 Generator Construction

The generator casing and end shields are of a welded, gas-tight construction. The gas-tight construction prevents the escape of the hydrogen gas used as the cooling medium. The casing houses and supports the stationary armature winding, the rotor, and the hydrogen gas coolers. Because the outer end shields are designed to support the weight of the rotor and prevent the escape of the hydrogen cooling gas, they contain the rotor bearings and the hydrogen shaft seals. The bearings are horizontally split, tin-base, babbitt-lined journal bearings. The hydrogen seals are located inboard of the bearings to allow bearing maintenance without gas evacuation of the generator. The bearing ring at the collector end is insulated from the end shield to prevent stray shaft electrical currents from circulating through the bearings. The bearings are forced-oil lubricated by the turbine-generator lube oil system. The inner end shields are located between the armature winding and outer end shields and serve to separate the cooling fan suction and discharge. Fan nozzles, attached to the inner end shields, provide optimum gas flow for the cooling fans.

6.7.1.2 Stator Core

The stator core is made up of segmented, insulated, silicon sheet steel with radial slots for installation of the stator bars. The core must be made of a high permeability steel so that it can easily pass the lines of flux. This feature reduces the amount of field current necessary to achieve the high terminal voltage. The reason several thin insulated sheets are used rather than a single section is to minimize circulating eddy currents within the core. Excessive eddy currents could lead to core overheating. After assembly, the core is varnished and baked for corrosion resistance and further insulation. The core is contained within the stator frame, which is made up of the casing and end shields.

6.7.1.3 Stator Winding

The armature winding is comprised of insulated bars of hollow copper strands joined at the ends to form coils and connected in the proper phase belts by connection rings. The copper strands are arranged in the form of a rectangular bar such that each strand shares an equal load current. This method of winding is accomplished by spiraling each strand along the entire bar length such that each strand occupies every radial position at some point in the bar. In addition to ensuring equal load current, this arrangement also minimizes current losses within the bar. Each bar is individually insulated with mica tape.

The individual hollow strands are joined at each end of the bar by a clip assembly forming a manifold. De-ionized water, used for cooling purposes, is supplied to one end of the winding by a flexible Teflon hose. The cooling outlet header is located on the opposite end of the winding. To prevent flux leakage from the end of the stator core to the retaining rings on the field, a copper flux shield is installed over the steel clamping flange at each end of the stator core. This tends to reduce losses in the end turns of the stator windings.

6.7.1.4 Rotor

The rotor is machined from a single steel forging. A center axial hole is drilled the length of the rotor to carry the leads from the collector rings to the field windings. Slots are machined radially in the rotor to contain the field coils. The field windings consist of rectangular bars formed into coils and held in place by textolite wedges. Several turns in one pair of slots around one pole form a coil, and several coils assembled around each pole (located 90° apart) form the field winding. The end turns of the winding are held in place on the rotor by retaining rings which are attached to centering rings on the rotor shaft. The turns of the windings have a series of holes for cooling purposes and are individually insulated. All turns are series wired and attached to the connection bars in the center bore hole of the shaft. These connections are made by terminal studs. Current is supplied to the field windings through self-lubricated graphite brushes that ride on collector rings installed on the end of the rotor shaft. Current then travels through additional terminal studs to the connection bars located in the shaft centerline. Each field-side and collector-side terminal stud is gasketed to prevent gas leakage.

6.7.2 Generator Cooling

All generator components, with the exception of the stator windings, are cooled by hydrogen gas. Hydrogen is chosen as the coolant because it is non-corrosive and has a high electrical resistance and a relatively high thermal conductively. It is also a low density gas, reducing windage and ventilating losses. The gas is circulated at 90,000 cfm by two fans, one mounted on each end of the generator and driven by the rotor. The gas is forced through the radial ducts in the core, removing the heat generated in the electrical production process, and is then circulated through four gas coolers and back to the suction sides of the fans. The rated hydrogen pressure is 75 psig; the minimum allowable pressure is 30 psig. The generator contains 5180 cubic feet of hydrogen at 98% purity.

High and low pressure areas are established within the frame by plates in the frame and back of the core and by the outside wrapper plate. Hydrogen is circulated through these areas by tubes and ducts. The four gas coolers are vertically mounted in the frame, one on each corner.

Any one cooler may be serviced with the generator at load. The coolers are supplied with water from the turbine building cooling water system.

Stator cooling is accomplished by deionized water from the stator cooling water system. The water is supplied to the clip assembly of each individual hollow strand and then into an annular header connected to the stator cooling water system.

6.7.3 Component Descriptions

6.7.3.1 Excitation System

The alternator-exciter produces the output current used by the main generator's field. It is a direct-coupled, four-pole, ac synchronous generator driven by the main generator rotor. Located on the end of the main generator, it has a construction similar to that of the main generator except that it is air cooled and self excited during operation. Two fans, mounted on either end of the alternator-exciter shaft, circulate filtered air throughout the exciter. Circulated air is cooled by heat exchangers mounted on top of the exciter housing. The heat exchangers are cooled by the turbine building cooling water system. The alternating current from the smaller ac generator (exciter) is rectified by a group of power rectifiers to furnish direct current for the main generator field.

As shown in Figure 6-9, generator excitation is controlled by varying the field current to the exciter. The exciter field excitation is controlled by a static voltage regulator. The regulator is a thyristor type containing silicon-controlled rectifiers (SCRs) in the output circuit that drives the exciter field. The regulator includes both automatic and manual control functions to regulate the generator terminal voltage or the generator field voltage, respectively.

The SCR control signal comes from the AC regulator or DC regulator as selected by the transfer panel. With the exciter operating in manual control, the DC regulator holds generator field voltage constant. With the exciter operating in automatic control, the AC voltage regulator holds generator terminal voltage constant. A transfer voltmeter is used for matching signals to provide for a smooth transfer between the two regulators.

6.7.3.2 DC Voltage Regulator

In DC voltage operation, the generator field voltage is sensed to control and keep the exciter output constant. The DC regulator consists of three basic elements. The front end senses exciter output voltage and compares it with a reference voltage to produce an error signal. The error signal is increased by the amplifier stage for the SCR bridge firing circuit. The controlling set point for the regulator is adjusted in the control room. The inputs to the DC regulator include a feedback signal from the exciter voltage and a current input to act as an auxiliary power source during transient conditions when the exciter voltage may be low.

6.7.3.3 AC Voltage Regulator

Alternator-exciter field excitation is controlled in the same way in both AC and DC operation. The AC regulator senses generator output terminal voltage to keep it constant under varying load conditions. The basic control system scheme is the one used in DC operation, with some major signal differences. The error signal produced by the front end is essentially the same, except that the AC regulator's range is more limited and the terminal voltage signal is compensated. A reactive current compensator (droop circuit), causes a decrease in the terminal voltage signal with an increase in generator reactive load. The terminal voltage signal is decreased as load increases, regardless of the voltage drop between generator and grid. A comparison circuit receives a compensated voltage signal, compares it to the reference voltage, and produces a compensated error signal. This signal is proceessed as described in the preceding section; the result is an output to the SCR bridge firing circuit.

6.7.3.4 Relaying and Control Circuits

Relaying and control circuits are operated by dc power, which is supplied from storage batteries for maximum reliability. The following control functions are provided:

1. field breaker
2. regulator transfer and lockout
3. exciter field bridge overcurrent
4. generator field bridge overcurrent
5. exciter field flashing
6. motor-driven DC regulator setpoint adjuster.

6.7.3.5 Generator Synchronizing Circuit

The synchronizing check relays ensure that the main generator output breakers close only when the main generator is synchronized to the grid. The synchrocloser relay (semi-automatic) controls the closure of the first output breaker to the grid. It provides a close signal to the breaker such that it will close when the synchroscope is at 0°, provided the following conditions are met:

1. The synchroscope is rotating at one to three rpm in the "fast" direction,
2. The switchyard voltage is between 218 and 249 kv,
3. The voltage differential between the generator and switchyard is within 10 kv, and
4. The breaker control switch is selected to "close."

The manual synchronizing relay (zero slip) controls the closure of the second output breaker when the slip frequency is zero, such as when the generator has been synchronized with the grid with the first output breaker. It provides a close signal to the breaker when the following conditions are met:

1. The phase angle is ± 10°,
2. A time delay of seven seconds has passed with slip frequency at zero (synchroscope stopped), and
3. The breaker control switch is selected to "close."

6.7.4 Main Generator Protection

6.7.4.1 Turbine Trips

A turbine trip will result in a generator trip (opening of the generator output breakers). Some turbine trips (in which there are no electrical faults which require tripping the generator from the network) allow a delay in generator tripping of 30 seconds. This delayed trip ensures that the reactor coolant pumps remain in operation for 30 seconds following the trip, ensuring an adequate coastdown time. The delay also helps to prevent an overspeed condition by using the steam that is still present in the valve chests, turbines, and moisture separator reheaters to generate some electrical power after the turbine inlet valves are tripped closed. Power from the grid is reversed through the main transformer to the unit auxiliary transformer supplying all auxiliary loads. When the generator trips, a fast transfer of the 12.47-kv buses to the startup transformers occurs, and power is maintained to the auxiliaries.

The following turbine trips allow a 30-second delay of the generator trip:

1. high steam generator level
2. low condenser vacuum
3. reactor trip/safety injection
4. low electrohydraulic control (EHC) hydraulic pressure
5. loss of EHC pressure
6. high turbine vibration
7. loss of 24 vdc/125 vdc
8. high exhaust hood temperature
9. underfrequency
10. overspeed.

The following turbine trips results in an immediate generator trip:

1. manual
2. backup overspeed
3. loss of two speed signals
4. thrust bearing wear/low oil pressure
5. loss of stator coolant
6. low shaft lube oil pump pressure
7. moisture separator drain tank level

6.7.4.2 Generator Lockout Relays

A generator lockout signal will trip the main turbine, the exciter breaker, the main generator output breakers, and the unit auxiliary transformer output breakers. It will also initiate a fast transfer of power to the startup transformers. Relays are energized to lock out the generator in the event of a generator, main transformer, or unit auxiliary transformer fault.

6.7.5 Main Transformer

The main transformer increases the line voltage of the generator output from 22 to 230 kv for distribution. By raising the line voltage, hysteresis and resistance losses are significantly reduced, thus minimizing conductor heating. The increased line voltage eliminates the need for costly bus cooling systems and reduces the expense of distribution systems. The main transformer is actually two transformers in parallel which receive power from the isophase buswork and, after raising the voltage to 230 kv, deliver it to the high voltage overhead transmission system. Each transformer can carry two-thirds of the total station generating capability.

Each transformer consists of three single-phase transformers. The high voltage winding is wye connected with a solid-grounded neutral, while the low voltage winding is delta connected. Each phase is a 22-to-230-kv, outdoor, oil-filled transformer rated at 535 Mva. The 230-kv power from the main transformers is transmitted by the overhead transmission system to the switchyard.

6.7.6 General System Operation

6.7.6.1 Normal Operation

During operation the voltage regulator is adjusted to maintain the proper reactive loading, and the DC regulator position is verified to be near that of the AC regulator. This allows a smooth transfer in case control is shifted to the DC regulator.

6.7.6.2 System Shutdown

At 20% load, the 12.47-kv buses are manually transferred from the unit auxiliary transformers to the startup transformers. When the reactor power is reduced to 5%, the turbine is tripped and the generator output and exciter field breakers trip open. The voltage regulator is placed in manual, excitation current is removed, and the unit is secured.

6.7.6.3 System Operations While Shutdown

The main generator output breakers can be cycled from the switchyard control house. Exercising the breakers should ensure that they will close in a timely manner prior to plant startup.

When a startup transformer is required to be removed from service, its 12.47-kv bus may be energized (backfed) via the main and unit auxilary transformers through the generator output breaker(s). The operators will be able to control the generator output breakers from the control room.

6.7.6.4 Generator Operating Limits

The operation of a generator involves certain limiting conditions. A generator has so many variable operating factors that the operating limits cannot be easily or simply specified. The purpose of the operating limits is primarily to protect the generator from excessive temperature. The capability or capacity of a generator is limited by the hot-spot temperatures in various elements of the component, such as the stator winding, rotor winding, and the stator iron, and by the temperature differential across the insulation of the winding. Any one of these points may be the limiting location depending on the load, power factor, etc. High temperature causes damage to the winding insulation which may lead to an internal fault. The insulation damage occurs from embrittlements due to the elevated temperature. Brittle insulation is subject to cracking and loss of its insulating properties. This type of damage is basically a result of the temperature existing at a point. Another type of temperature-related damage occurs from the differential expansion between the winding conductors and the core. The thermal expansion causes relative movement with resultant abrasion and damage to the insulation.

The heat produced in the generator or any other electrical apparatus is a function of the current and the resistance (I^2R). As current increases, the amount of heat produced increases rapidly due to the current squared term. This heat must be removed by the cooling medium (either hydrogen gas or liquid).

In the newest and largest generators another factor, other than temperature, is becoming important in prescribing operating limits. Electromagnetic forces acting on various components of the generator are now of significance. The large capacity of such a generator produces magnetic fields of great strength. These strong fields are constantly revolving and apply fluctuating forces to the generator components. Movement induced by these forces can cause vibration and eventual failure of components which are not properly restrained.

There are other factors that play important roles in limiting the operation of a generator. These are rotor vibration, generator frame distortion, and reactive capability limits.

Vibration of the rotor due to imbalance does not constitute an electrical problem. It may, however, cause damage to bearings and/or seals. A typical limit is five mils.

The reactive capability curve defines the operating limits which ensure that hot-spot temperature conditions are not excessive. The curve is based on design and test information and includes allowances for manufacturing tolerances.

The basic limitation is on the apparent power in Mva (mega-volt-amperes), not on the true power in Mw. The heating effect of current is independent of whether the current is in or out of phase with the voltage. If the basic limitation is Mva rating and the voltage is relatively constant, then the limit is essentially governed by the generator current over a limited operating range. It is sometimes desirable to operate the generator at power factors considerably different from unity. For this type of operation, the use of a reactive capability curve is essential.

6.7.7 Summary

The main generator produces electrical power and transmits that power to the offsite distribution system. The generator output voltage is stepped up from 22 kv to 230 kv by the main transformer for delivery to the high voltage overhead transmission system. It also supplies power for normal operation of station equipment.

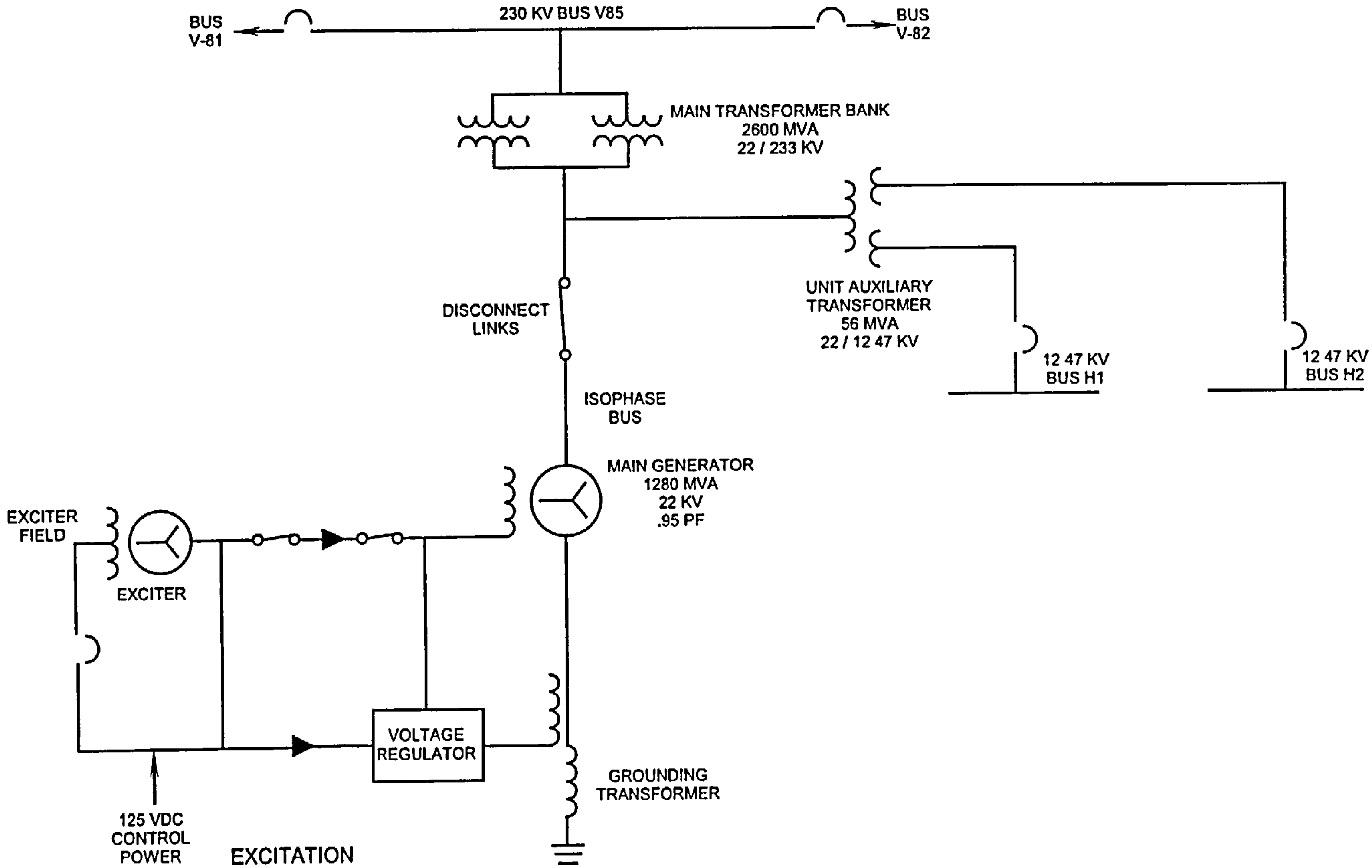


Figure 6-9 Main Generator Schematic

0199-3

8.4 ROD INSERTION LIMITS

Learning Objectives:

1. State the purposes of the control rod insertion limits (RILs).
2. List the inputs into the rod insertion limit computers and comparators.
3. Explain why the rod insertion limits increase with increasing reactor power.

8.4.1 Introduction

The rod insertion limits ensure that the control rods are sufficiently withdrawn to:

1. Maintain an adequate shutdown margin,
2. Maintain nuclear peaking factors within limits, and
3. Minimize the reactivity effects on the core due to an ejected rod.

The rods may only be inserted a certain number of steps into the core for a specific power level. The limiting conditions for operation (LCO) of the plants technical specifications address this limit. These limits ensure that the rods can place the reactor in the hot shutdown condition following a reactor trip. This chapter discusses the assumptions, considerations, and calculations used to determine the rod insertion limits.

8.4.2 System Description

8.4.2.1 Assumptions and Considerations

The rod insertion limits ensure that there is enough negative reactivity associated with the rods to place the reactor in the hot shutdown condition following a reactor trip with the following assumptions:

1. The highest worth rod is stuck full out. With the highest worth rod stuck in the fully withdrawn position, the negative reactivity associated with this rod will not be available to shutdown the reactor.
2. The reactor is operating with the highest power defect (Section 2.1). This assumes that the core is operating at full rated thermal power, and the reactor is at the end of life (EOL).
3. The plant is operating with the highest deviation from rated T_{avg}.

These assumptions reflect the assumptions used in the accident analysis section of the final safety analysis report (FSAR). Besides these assumptions, the Westinghouse design criteria for the rod insertion limits, stipulate that there is not a return to criticality following the opening (fails open) of an atmospheric steam relief, a code safety valve on a steam generator, or a steam dump valve. This single failure causes a rapid cooldown of the reactor coolant, which adds positive reactivity to the core. Failing open any one of these valves affects plant safety similar to that of a small steam line break equivalent to 247 lbm/sec loss of secondary inventory. A steam break of this size is an analyzed accident and it is categorized as a condition III event in the FSAR.

The rod insertion limits must meet the above assumptions, and this section will examine some additional considerations. First, setting the insertion limit as low as possible is desirable (rods greatly inserted into the core) to allow the largest range of rod motion for power maneuvering. Finally, setting the insertion limit as high as possible is desirable (rods barely inserted into the core) to ensure that the nuclear peaking factors are maintained. Remember inserting the rods into the core, changes the neutron flux distribution. Changing the flux distribution within the core could have an adverse effect on the nuclear peaking factors. Therefore, withdrawing the rods from the core minimizes this effect. In addition, the high withdrawal setpoint reduces the positive reactivity addition consequences of a hypothetical rod ejection accident.

The setpoint selection of the rod insertion limit meets the requirements of the assumptions stated at the beginning of this section (8.4.2.1), and the insertion limit allows the rods to operate at an optimum point between the requirements for plant maneuverability and the requirement to maintain the nuclear peaking factors.

8.4.3 Component Description

8.4.3.1 Rod Insertion Limit Computer

Consider what happens as reactor power increases. As the power in the core increases, the following reactivity coefficients, Doppler, moderator temperature, and void fraction, add negative reactivity to the core. To maintain the criticality of the core the reactor operator must add an equal amount of positive reactivity. Positive reactivity addition can be accomplished via control rod withdrawal, boron dilution or a combination of the two.

The power defect is the sum of these reactivities and is the total amount of reactivity added to the core due to a power change. Therefore, when a reactor trip occurs, the moderator temperature, fuel temperature, and void fraction add positive reactivity to the core. The power defect is now adding positive reactivity to the core. To ensure there is sufficient negative reactivity associated with the shutdown and control rods to shutdown the reactor following a trip, the rod insertion limits increase as reactor power (and power defect) increase.

Two parameters, proportional to power, are used as inputs to the rod insertion limit computers (Figure 8.4-1). These parameters are, auctioneered high ΔT and auctioneered high T_{avg}. They were selected because ΔT is a direct function of power, and T_{avg} is programmed as a function of power. The auctioneering units select the highest values of ΔT and T_{avg}. Therefore, the calculation of the rod insertion limit assumes a conservatively high representation of power. The rod insertion limit computers calculate the insertion limit for selected control rod banks using the following equation:

$$RIL = K_1\,(T_{avg}\text{-}557\,°F) + K_2\,(\%\Delta T) + K_3$$

Where:

1. RIL = the maximum permissible rod insertion limit for a selected control bank

2. K_1 is a constant used to compensate for the effect of the moderator temperature coefficient if the plant is operating at a higher temperature program than the design T_{avg} program. If a plant is operating with an escalated T_{avg}, the extra reactivity associated with the greater cooldown of the reactor coolant following a reactor trip must be accounted for. Most plants operate within their normal programmed T_{avg} band; therefore, the normally assigned value for K_1 is zero.

3. (T_{avg} - 557°F) = the highest auctioneered T_{avg} minus the no-load T_{avg} (557°F)

4. K_2 accounts for power defect. Since the auctioneered high ΔT varies directly with power, the constant K2 (expressed in steps per $\%\Delta T$) times the $\%\Delta T$ results in a given number of rod steps. This factor ensures that

the calculated rod insertion limit provides enough negative reactivity to place the plant in the hot shutdown condition from any power level. (Note: K_2 is the slope of the RIL shown on Figure 8.4-2.)

5. (%ΔT) = the highest auctioneered ΔT in percent power ΔT. The expected ΔT for 100% power is approximately 64°F. Therefore, the input to the rod insertion limit computer at full power would be 100, i.e., ([64/64]x100). If the ΔT across the core is 32°F, then the input to the rod insertion limit computer would be 50, i.e., ([32/64]x100)

6. K_3 provides the minimum insertion limit set point for hot zero power, i.e., the minimum insertion for criticality. K_3 ensures that the negative reactivity associated with the rods at this limit places the reactor into hot shutdown assuming the worst case conditions (EOL in conjunction with a rapid cooldown associated with the previously mentioned small steam break). K_3 is the Y intercept of the RIL shown on Figure 8.4-2.

The values for these constants vary depending upon, plant design, fuel loading, fuel design, and rod worth. These values can be found in the Precautions, Limitations, and Setpoints (PLS) document for each Westinghouse plant. A typical set of constants and their respective values (where the value of K equals steps) is listed below:

	K_1	K_2	K_3
Control Bank C	0	1.99	118
Control Bank D	0	1.99	- 10

Figure 8.4-2 displays the rod insertion limit for different control banks versus reactor power.

For example, calculations for the rod insertion limits for control banks C and D with plant at 50% power are shown below:

CONTROL BANK C

RIL = K_1 (T_{avg} - 557°F) + K_2 (%ΔT) + K_3
RIL = 0 (571°F - 557°F) + 1.99 (50) + 118
RIL = 0 + 99.5 + 118
RIL = 217.5 steps on Bank C

CONTROL BANK D

RIL = K_1 (T_{avg} - 557°F) + K_2 (%ΔT) + K_3
RIL = 0 (571°F - 557°F) + 1.99 (50) + (- 10)
RIL = 0 + 99.5 - 10
RIL = 89.5 steps on Bank D

After the computer calculates the insertion limit for the selected control banks, the calculated limit is sent to the RIL comparator circuit.

8.4.3.2 Rod Insertion Limit Comparator

The rod insertion limit comparator receives two input signals for comparison. The first input comes from the rod insertion limit computer, which calculates the rod insertion limit. The second input comes from the pulse to analog converter (Section 8.2). This input represents demanded rod position. The rod insertion limit comparator compares the calculated rod insertion limit to the demanded rod position. If the demanded position is within a preselected value of the limit or if the two inputs are equal, annunciators inside the control room alarm. The alarms generated by this comparator are "Rod Insertion Limit Low" and "Rod Insertion Limit Low Low." The equations for each of these alarms are shown below:

- RIL Low = RIL + 10 steps
- RIL Low Low = RIL

As written above, two alarms can be generated by each comparator. The purpose of these alarms is to provide the reactor operator with a warning of excessive rod insertion. Each alarm requires a specific action to be taken by the operator.

The "RIL Low" alarm alerts the operator of an approach to the rod insertion limit. In this case the operator is directed to add boron to the reactor coolant system according to the plants' normal operating procedures. The makeup portion of the chemical and volume control system (Section 4.1) is used to add boron to the reactor coolant.

The "RIL Low Low" alarm alerts the operator that the rods are at, or have exceeded, the Technical Specification limit. The operator has an option of either calculating the shutdown margin within one hour or borating the reactor coolant to restore the shutdown margin. In addition, within two hours of entry into this limiting condition of operation, the control bank/s must be moved to within their limit/s. This action, depending upon the plant's operating procedures, may have the control room operators' emergency borate (Section 4.1) or reduce thermal power to meet the minimum insertion limit.

8.4.4 Summary

The rod insertion limits are a Technical Specification LCO placed on how far the control rods may be inserted into the core. These limits ensure that there is sufficient shutdown reactivity associated with the rods to place the core in the hot shutdown condition following a reactor trip. The rod insertion limit computer continuously monitors its inputs (ΔT and T_{avg}) and calculates an insertion limit. The calculated insertion limit is compared with the demanded rod position and the resultant information is sent to control room annunciators and to a recorder on the main control board. The annunciators alert the reactor operator of an approach to a reduced shutdown reactivity condition.

10.3 PRESSURIZER LEVEL CONTROL SYSTEM

Learning Objectives:

1. State the purposes of the pressurizer level control system.

2. List and describe the purposes (bases) of the protective signal provided by pressurizer level instrumentation.

3. Identify the instrumentation signal that is used to generate the pressurizer level program, and explain why level is programmed.

4. Explain how charging flow is controlled in response to pressurizer level error signals during the following:

   a. Centrifugal charging pump operation
   b. Positive displacement charging pump operation.

5. Explain the purposes of the pressurizer low level interlocks.

10.3.1 Introduction

The purposes of the pressurizer level control system are to:

1. Control charging flow to maintain a programmed level in the pressurizer.

2. Provide inputs to pressurizer heater control and letdown isolation valves for certain pressurizer level conditions.

10.3.2 System Description

During steady state operation, an unchanging pressurizer level indicates that a balance exists between the charging flow into the reactor coolant system and the letdown flow from the reactor coolant system into the chemical and volume control system. During transients the level in the pressurizer changes because the reactor coolant expands or contracts as the average temperature of the coolant increases or decreases.

Designing a control system to maintain a constant pressurizer level, as reactor power and reactor coolant temperatures change, is a relatively simple matter. However, a major disadvantage of such a system is that, as the temperature of the reactor coolant increases, the coolant expands. The expansion of coolant is seen as an increase in pressurizer level. When the level in the pressurizer increases above the programmed setpoint, the pressurizer level control system decreases the charging flow.

Recall from the Chemical and Volume Control System (section 4.1) that the amount of letdown flow from the reactor coolant system is constant (75 gpm). Knowing this fact and with the information provided in the previous paragraph, the amount of coolant being letdown is greater than the amount of coolant being returned to the reactor coolant system via the charging pumps. With this imbalance of flow, the level in the volume control tank increases. When the level in the volume control tank reaches a high level, coolant is diverted to the holdup tanks.

Once the water is diverted, it is treated as liquid waste and is processed for reuse. This places a large burden on the liquid radioactive waste processing systems.

On the other hand, a decrease in the temperature of the reactor coolant causes the coolant to contract and places a large demand on the makeup system. To minimize the demands on the liquid waste system and the chemical and volume control system, the level in the pressurizer is programmed to follow the natural expansion or contraction of the reactor coolant as temperature of the coolant increases or decreases.

The pressurizer level control system is shown in Figure 10.3-1, while the functional system parameters are displayed in Figure 10.3-2.

10.3.3 Component Description

10.3.3.1 Level Transmitters

The level in the pressurizer is measured by, comparing the difference in pressure between an external column of water of a known height (reference leg) and a variable unknown height of water inside the pressurizer (variable leg). The differential pressure (d/P) between these two columns of water is converted into a pressurizer level signal.

There are four differential pressure transmitters (d/P cells) mounted on the pressurizer. These d/P cells convert the sensed d/P into an electrical current that corresponds to a level varying from 0 to 100%. These transmitters utilize an external bellows type sealed reference leg with a condensate pot attached at the top of the leg to generate the static pressure head of the reference leg, and the actual water level inside the pressurizer to generate the dynamic or variable leg. Since the density of water varies with temperature, any temperature change of the coolant inside the pressurizer affects its indicated level. Therefore, the pressurizer level instruments are calibrated based upon pressurizer temperature.

Three of the four level transmitters are calibrated for normal operating temperatures and are used for indication, control and protection. The remaining level transmitter is calibrated for cold conditions and is used only for indication while operating at cold shutdown or when establishing a steam bubble in the pressurizer. The cold calibrated transmitter does not provide an input to the pressurizer level circuitry or an input into the reactor protection system.

The output of these level transmitters indicates a level from 0 to 100% inside the pressurizer. A selector switch, located on the main control board, allows the control room operator to select two of the three transmitters used for control. One channel is used for level control, letdown isolation, and pressurizer heater cutoff, while the other channel is used for backup letdown isolation, and heater cutoff. The third channel can be selected to replace either of the two controlling channels during testing or failures. An additional selector switch is provided on the main control board that allows the control operator to select any one of the three transmitters for recording.

10.3.4 System Interrelationships

10.3.4.1 Control Channel

The difference between the actual pressurizer level and the programmed reference level signal is supplied to the master pressurizer level controller. If an error signal exists, this PI (proportional plus integral) controller varies the chemical and volume control system charging flow. This controller prevents the charging flow from reacting to small temporary level perturbations while eliminating steady-state level errors. Since the letdown flow is fixed, the inventory balance of the reactor coolant system is maintained by varying the charging flow. This is accomplished by one of two different methods:

1. If the positive displacement charging pump is operating, charging flow is controlled by varying the speed of the positive displacement charging pump. For this method of control, the output of the master level controller is supplied to a proportional (P) pump speed controller.

2. If a centrifugal charging pump is operating, charging flow is controlled by varying the position of the flow control valve (FCV-121), located in the common discharge header downstream of the centrifugal charging pumps. For this method of control, the output of the master pressurizer level controller serves as the flow setpoint which is compared to the actual charging flow measured by flow transmitter FT-121, located just downstream of FCV-121. The difference is supplied to the PI charging flow controller, which controls the air pressure to the operator for FCV-121 and thus regulates its position. As FCV-121 is an air-to-close valve, an increasing output from the charging flow controller (meaning that charging flow exceeds the demand from the master level controller) repositions the valve in the closed direction.

When the plant is operating and the power in the reactor is changed, the average temperature of the reactor coolant system is programmed to change. This change in temperature causes a corresponding change in the level of the pressurizer. To reduce the effect on the charging system, the level in the pressurizer is programmed (shown in Figure 10.3-2), as a function of auctioneered high T_{avg} which corresponds to the natural expansion characteristics of the reactor coolant. However, rapid transients cause an increase or decrease in the level of the pressurizer which requires changes in charging flow. For this reason, both minimum and maximum level limitations are placed on the level program in order to prevent the following:

1. The pressurizer low level setpoint of 25% is selected to prevent the pressurizer from going dry following a reactor trip. In addition, this level; ensures that a step load increase of 10% power will not uncover the heaters.

2. The pressurizer high level setpoint of 61.5% is derived from the natural expansion of the reactor coolant when the coolant is heated up from no load to full power T_{avg} (557°F to 584.7°F), with the assumption that the level in the pressurizer was at 25% when the heatup began.

This level setpoint (61.5%) is lower than some maximum calculated level value, which ensures that the pressurizer does not go solid following a turbine trip from 100% power without a direct reactor trip, assuming no operator action, and no response by the automatic control systems (rod control and the steam dump system).

In addition this level 61.5%, is low enough so that the insurge from a step load reduction of 50% will not cause the level in the pressurizer to reach the high level reactor trip setpoint. This assumes the automatic rod control system and the steam dump system respond to the transient properly.

In general, an outsurge of water from the pressurizer results in a system pressure decrease and an insurge of water from the reactor coolant system results in a pressure increase. However, if the insurge is large, it results in a system pressure decrease because the insurge water is cooler than the water in the pressurizer. Therefore, if the level in the pressurizer increases above the program level setpoint by 5%, the control system automatically energizes the backup heaters in an effort to offset the above effect.

This may be observed on a step load decrease (RCS temperature increases due to reactor power being higher than the secondary load), which causes an initial insurge into the pressurizer, and the cooler water entering the pressurizer causes a pressure reduction. This insurge is followed by a larger outsurge as the rod control system brings T_{avg} to program for the lower power level which in turn causes a pressure reduction. Therefore, the 5% deviation above set setpoint serves as an anticipatory signal to limit the pressure reduction in the reactor coolant system upon a load decrease.

The same level signal which is compared to the reference level in the level controller is also sent to a bistable. This bistable provides a low level interlock and is set to actuate at 17% level in the pressurizer. In addition to providing a low level alarm, this interlock isolates the letdown from the chemical and volume control system by closing one letdown isolation valve and all orifice isolation valves, and turns off all pressurizer heaters. Isolating the letdown prevents further lowering of pressurizer level, and the heater cutoff protects the heaters which would be damaged if operated in a steam environment.

10.3.4.2 Redundant Isolation Channel

This channel consists of an actual level signal sent through the channel selector switch and then to two bistables. One of these bistables functions to provide a high level alarm at 70% level. The other bistable closes the second letdown isolation valve, provides a redundant signal to close all orifice isolation valves, and turns off all heaters.

10.3.4.3 Pressurizer High Level Reactor Trip

If two out of the three level transmitters sense a level greater than 92%, a reactor trip signal is generated. This trip is provided to protect the RCS pressure boundary, and trips the reactor before the pressurizer completely fills with water, "goes solid". It also functions as a backup to the high pressurizer pressure reactor trip.

The high level trip setpoint is selected at a value that is low enough so that the discharge of water through the pressurizer safety valves is prevented. This is important because water discharged through these valves does not relieve the overpressure condition as effectively as steam. Steam releases more BTU's of energy per pound mass than water. Also, discharges of water could mechanically damage the pressurizer safety valves.

This trip is an "at power" trip and is only active if either reactor power or turbine power is 10% or greater ("At Power Permissive" P-7). This reactor trip is discussed in detail in Chapter 12.

10.3.5 Summary

The pressurizer level control system maintains the water inventory of the reactor coolant system by varying the charging rate from the chemical and volume control system. In addition, provisions are made to isolate letdown and turn off the pressurizer heaters on a pressurizer low level. This feature minimizes the effects of a loss of coolant and protects the pressurizer heaters.

The system also turns on the pressurizer heaters if the level in the pressurizer is higher than the program level. Turning on the heaters is performed in anticipation of a pressure decrease following a loss of load transient.

A pressurizer high-level reactor trip is provided to prevent operation with a "solid" pressurizer and is incorporated into the reactor protection system for RCS boundary protection.

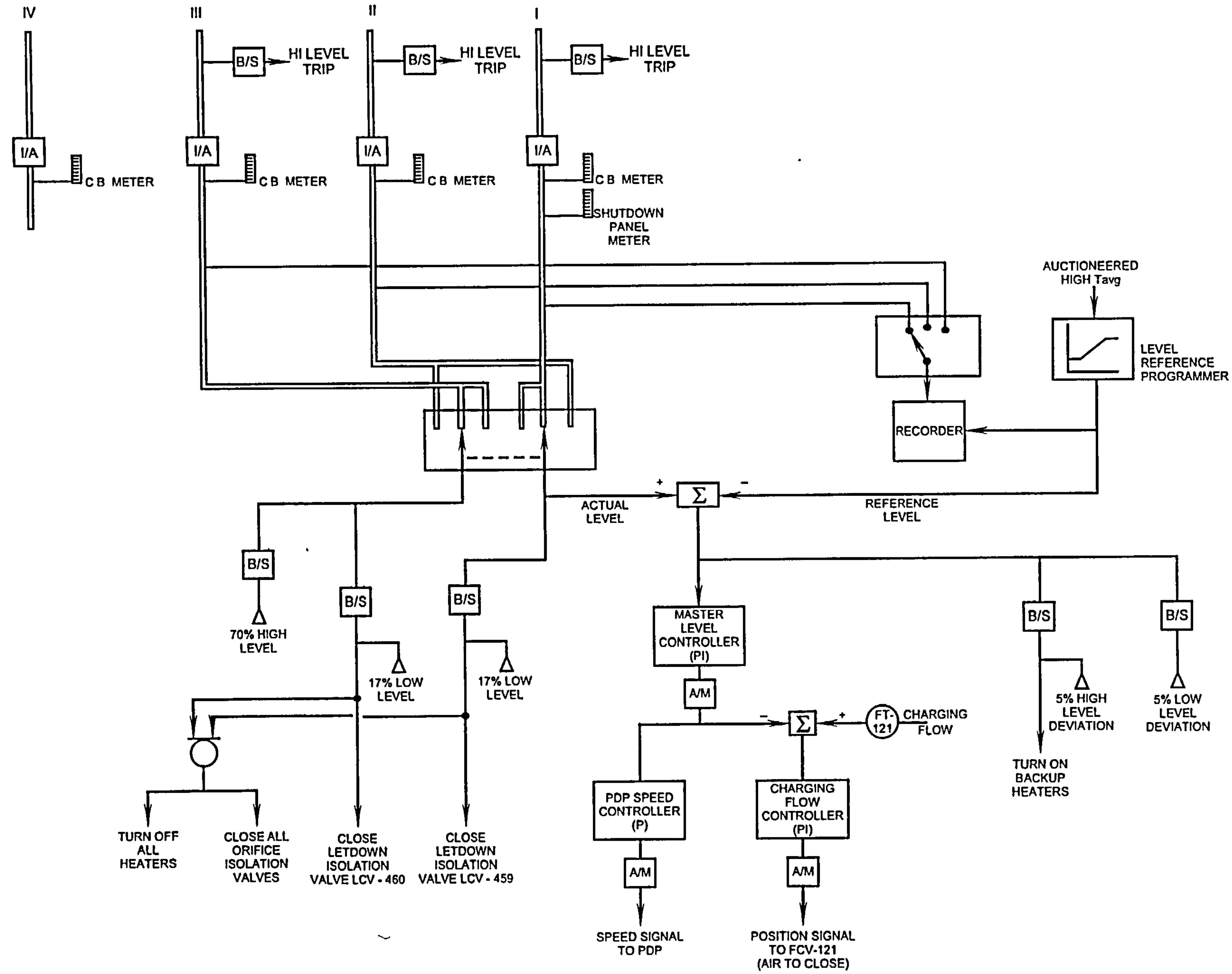


Figure 10.3-1 Pressurizer Level Control

2-3 3 A-8

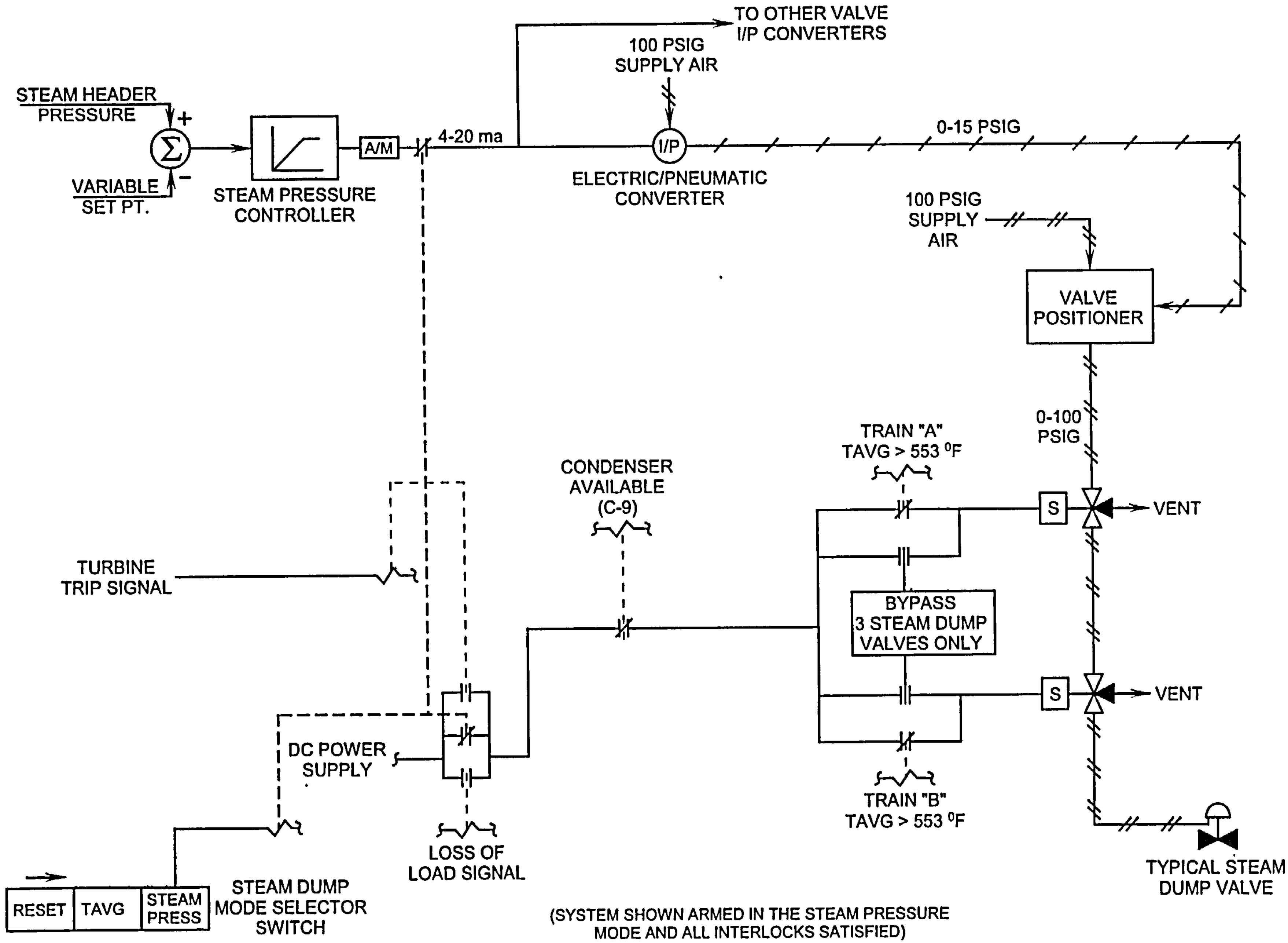


Figure 11.2-1 Steam Pressure Control Mode

0102-325
11-2-34-4

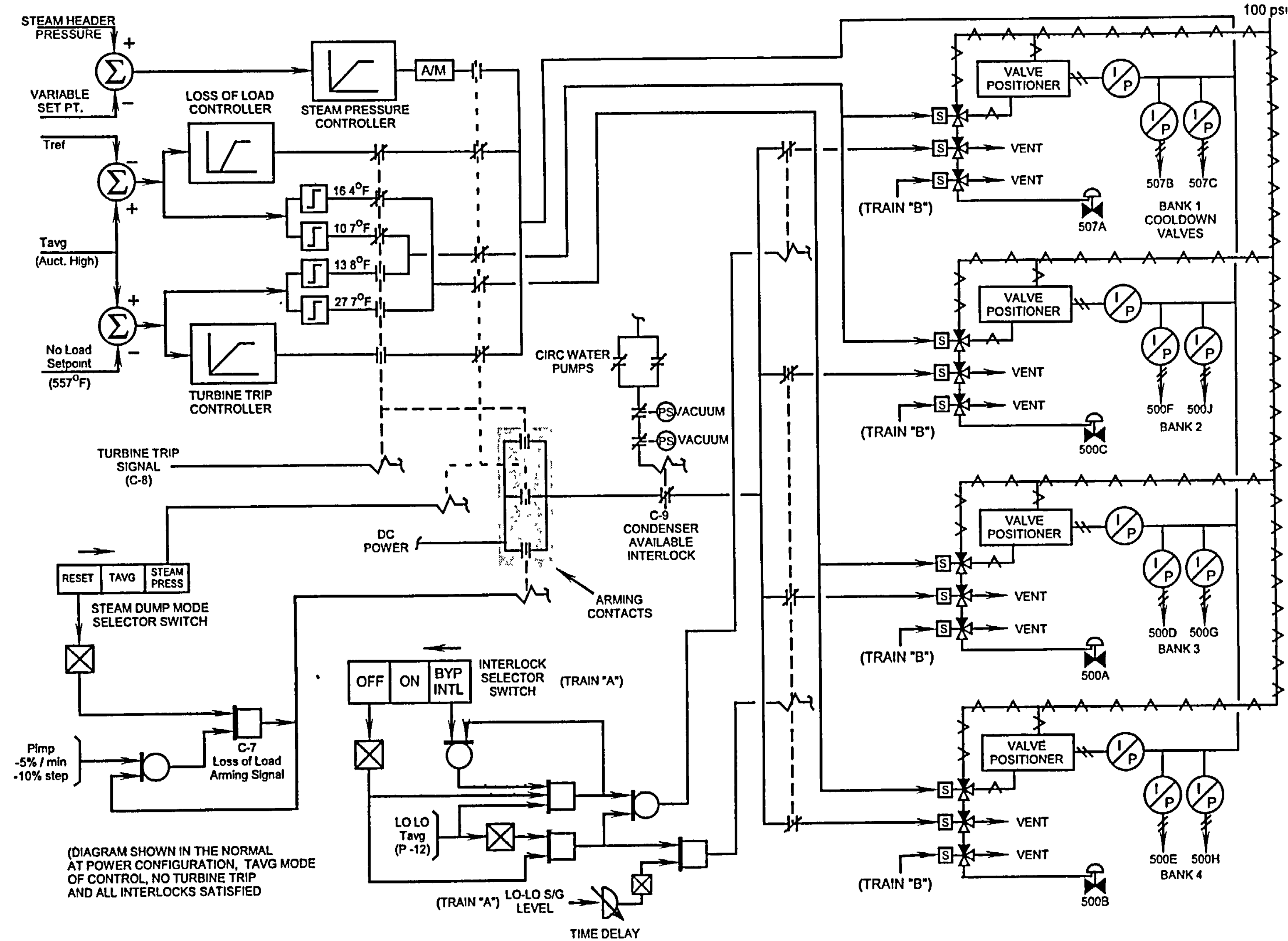


Figure 11.2-4 Steam Dump Control

0202-356
2-9 9

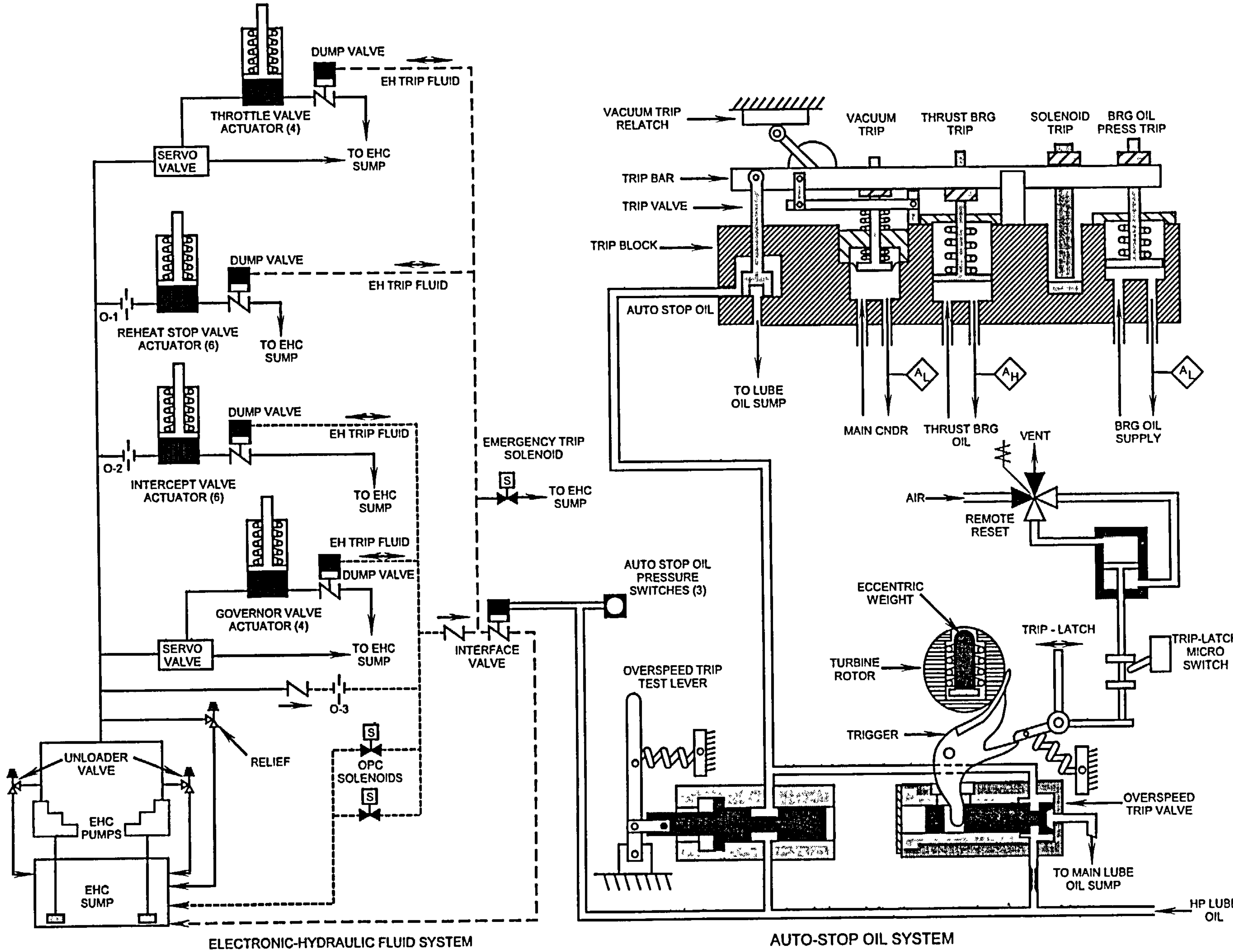


Figure 11.3-2 EH Fluid and Auto - Stop Oil System

0502-3

If three of four (3/4) power range channels drop below 10 percent power, the low power trip function is automatically reinstated. The high trip setting is always active (cannot be blocked). Prior to reaching the 109% trip setpoint a signal is generated to block automatic and manual rod withdrawal. This action occurs if any one of the four power range channels exceeds 103% power.

12.2.3.5 Positive Neutron Flux Rate Trip Power Range

This circuit, Figure 12.2-5, trips the reactor when an abnormal rate of increase in nuclear power (+5% with a 2 second time constant) occurs in two of four (2/4) power range channels. This trip provides protection for rod ejection accidents and cannot be bypassed or blocked.

12.2.3.6 Negative Neutron Flux Rate Trip Power Range

This circuit, Figure 12.2-5, trips the reactor when an abnormal rate of decrease in nuclear power (-5% with a 2 second time constant) occurs in two of four (2/4) power range channels. This trip provides protection against dropped rod accidents and cannot be bypassed or blocked.

12.2.3.7 Overtemperature ΔT Reactor Trip

The OTΔT trip, Figure 12.2-6, is designed to protect against departure from nucleate boiling (DNB) which causes a large decrease in the heat transfer coefficient between the fuel rods and the reactor coolant, resulting in high fuel clad temperatures. The indicated loop ΔT is used as a measure of reactor power and is compared with a continuously calculated trip setpoint. This setpoint is a function of Tavg, pressurizer pressure and axial flux difference. If the indicated ΔT equals the calculated trip setpoint, the affected channel is tripped.

If two or more channels are simultaneously tripped, the reactor is automatically shutdown. A turbine runback occurs and both automatic and manual rod withdrawal are inhibited at a ΔT value 3% below the trip setpoint. The equation for the calculation of the OTΔT setpoint is:

$$\text{OT}\Delta\text{T setpoint} = \Delta T_0\left[K_1 - K_2\left(\frac{1+t_1 S}{1+t_2 S}\right)(T - T') + K_3(P - P') - f_1(\Delta I)\right]$$

where:

ΔT_0 = (Indicated ΔT at RATED THERMAL POWER)

T = (Average temperature, °F)

T' = (Indicated T_{avg} at RATED THERMAL POWER)

P = (Pressurizer pressure, psig)

P' = (2235 psig, RCS nominal operating pressure)

K_1 = (a manually adjusted preset bias that sets the steady state trip point when the other parameters are at their rated values)

K_2 & K_3 = (manually adjusted preset gains)

$\left(\frac{1 = t_1 S}{1 = t_2 S}\right)$ = (The lead - lag function generated by the controller for the dynamic response of T_{avg})

t_1 & t_2 = (The time constants utilized in the lead - lag controller)

S = (Laplace transform operator)

$f_1(\Delta I)$ = (A function of the indicated difference between the top and bottom detectors of the nuclear power range instruments)

The Tavg term in the equation acts to lower the trip point when above normal full power Tavg. This is necessary because the increased average temperature reduces the margin to DNB. The pressure signal reduces the ΔT setpoint when pressure is lower than rated since this condition reduces the margin to DNB. The $f(\Delta I)$ term reduces the value of the trip point to reflect an increase in the hot channel factors which could result in localized DNB. The best axial flux distribution is a cosine function and results in equal power production in the upper and lower portions of the core. Any deviation from this shape is sensed by a difference between the upper and lower power range detector channels. This difference is referred to as axial flux difference or ΔI and is used to generate an output which reduces the trip setpoint. This insures DNB limits are not exceeded even for highly skewed power distributions. The OTΔT trip ensures that the DNBR not less than 1.30 at the time of the reactor trip if:

- The transient is slow with respect to piping transient delays from the core to the temperature detectors and
- The reactor coolant pressure is within the bounds set by the high and low pressure trips.

Prior to the actual ΔT reaching the OTΔT trip setpoint, both automatic and manual control rod withdrawal is inhibited and a cyclic turbine runback is initiated as long as the overtemperature condition exists. This action occurs if two of the four channels are within 3% of design full power ΔT of the trip setpoint.

12.2.3.8 Overpower ΔT Reactor Trip

The OPΔT trip , Figure 12.2-7, is designed to protect against a high fuel rod power density (excessive kw/ft) and subsequent fuel rod cladding failure and fuel melt. This is avoided by limiting fuel centerline temperature to less than 4700°F, which is significantly below the actual UO_2 melting temperature. The indicated ΔT is used as a measure of reactor power and is compared with a setpoint that is automatically calculated as a function of Tavg and axial flux difference. If the ΔT signal exceeds the calculated setpoint, the affected channel is tripped. If two or more channels are tripped simultaneously, the reactor is tripped. A turbine runback occurs and both automatic and manual rod withdrawal is inhibited at a ΔT value 3% below the OPΔT trip point. Since core thermal power is not precisely proportional to ΔT due to the effects of changes in coolant density and heat capacity, a compensating term which is a function of average temperature is used. Similarly, since the prescribed overpower limit may not be adequate for highly skewed axial power distributions, a compensating term related to ΔI is used. The setpoint equation is:

OPΔT setpoint =

$$\Delta T_0\left[K_4 - K_5\left(\frac{t_3 S}{1+t_3 S}\right)T - K_6\left(T - T'\right) - f_2\left(\Delta I\right)\right]$$

where:

$$\Delta T_0 = \left(\begin{array}{l}\text{Indicated } \Delta T \text{ at RATED}\\ \text{THERMAL POWER}\end{array}\right)$$

$$T = \left(\text{Average temperature, } {}^{0}\text{F}\right)$$

$$T' = \left(\begin{array}{l}\text{Indicated Tavg at RATED THERMAL}\\ \text{POWER} \le 584.7\ {}^{0}\text{F}\end{array}\right)$$

$$\frac{t_3 S}{1+t_3} = \left(\begin{array}{l}\text{The function generated by the rate}\\ \text{lag controller for Tavg dynamic}\\ \text{compensation}\end{array}\right)$$

$$t_3' = \begin{pmatrix}\text{The time constant utilized th the} \\ \text{rate lag controller for Tavg}\end{pmatrix}$$

$$S = (\text{Laplace transform operator})$$

$$f_2(\Delta I) = \begin{pmatrix}\text{A function of the indicated} \\ \text{difference between the top and} \\ \text{bottom detectors of the power} \\ \text{range ion chambers}\end{pmatrix}$$

$$K_4 = \begin{pmatrix}\text{A manually adjusted preset bias that} \\ \text{sets the steady state trip point when} \\ \text{the other parameters are at their rated} \\ \text{values}\end{pmatrix}$$

$$K_5 \,\&\, K_6 = (\text{Manually adjustable preset gain})$$

The T - T' term represents an upper limit of the equation which is based upon full power. Since it is possible for the average temperature to exceed the programmed full power average temperature, the setpoint must be reduced to take into account the increase in the heat capacity of the reactor coolant at higher temperatures. This term can only decrease the ΔT setpoint from its normal full power value. Prior to the actual ΔT reaching the OPΔT trip point, both automatic and manual control rod withdrawal is inhibited and a cyclic turbine runback will be initiated as long as the overtemperature condition is present. This action occurs if two of the four channels are within 3% of the setpoint.

12.2.3.9 Pressurizer Low Pressure Trip

The pressurizer low pressure trip, Figure 12.2-8, protects against excessive core steam voids and limits the range of required protection afforded by the OTΔT trip. The reactor trips when two of four (2/4) pressurizer pressure signals fall below 1865 psig. This trip is automatically blocked when turbine first stage pressure or reactor power are less than approximately 10 percent power (P-7).

12.2.3.10 Pressurizer High Pressure Trip

The high pressurizer pressure trip protects against reactor coolant system over pressure, thereby protecting the RCS pressure boundary. As shown in Figure 12.2-9, the reactor trips when two of four (2/4) high pressurizer pressure signals exceed 2385 psig. This trip is always in service and cannot be bypassed or blocked.

12.2.3.11 Pressurizer High Water Level Trip

The pressurizer high water level trip, shown in Figure 12.2-10, is provided to prevent rapid thermal expansions of reactor coolant fluid from filling the pressurizer and causing an over pressurization of the reactor coolant system. In addition a change from relieving steam to water could be damaging to the relief and safety valves. The reactor is tripped when two of three (2/3) high pressurizer water level signals exceed 92% level. This trip is automatically blocked below 10 percent power (P-7).

12.2.3.12 Low Reactor Coolant Flow Trip

The low flow reactor trips protect the core from DNB following a loss of coolant flow. The methods of sensing a loss of reactor coolant flow are shown in Figure 12.2-11 and described below:

a. Low primary coolant flow trip: A low loop flow signal is generated by two-out-of-three low flow signals per loop. Above the P-7 setpoint (approximately 10% of full power), a low flow in two or more loops results in a reactor trip. Above the P-8 setpoint (approximately 39% of full power) low flow in any single loop results in a direct reactor trip.
b. Reactor coolant pump breaker position trip: Each reactor coolant pump breaker supplies a

signal to the logic section of the reactor protection system. Above the P-8 setpoint, the reactor trips if any single reactor coolant pump breaker opens.

c. Reactor coolant pump under-voltage trip: The RCP under-voltage trip anticipates and improves the response of the RPS to a complete loss of reactor coolant flow. Each of the two RCP busses is equipped with two under-voltage sensors. An under-voltage condition, as sensed by one of two (1/2) devices on the bus, must exist on two of two (2/2) RCP busses to produce a reactor trip.

d. Under-frequency trips: An under-frequency condition on the RCP busses reduces the speed of the pumps (with a subsequent reduction in flow). This is undesirable because it reduces the coast down of the pumps if power is lost to the busses. Each of the two RCP busses is equipped with two under-frequency sensors. An under-frequency condition as sensed by one of two (1/2) devices on the bus, must exist on two of two (2/2) RCP busses to produce a reactor trip. In addition to tripping the reactor; if an under-frequency condition exists, a signal is sent to trip the RCP breakers

Note: All the reactor coolant low flow trips are automatically blocked below the P-7 setpoint (10% power).

12.2.3.13 Low Feedwater Flow Trip

The low feedwater flow trip, Figure 12.2-12, protects the reactor from a loss of primary heat sink. The trip is actuated by the logic of a steam flow greater than feed flow mismatch signal coincident with a steam generator low level.

12.2.3.14 Low-Low Steam Generator Water Level Trip

This trip (Figure 12.2-13) protects the reactor against a loss of heat sink. The setpoint of this trip is 11.5% as indicated on the narrow range indicators and is actuated on two of three (2/3) low-low water level signals in any single steam generator.

12.2.3.15 Engineered Safety Features Actuation Trip

If a reactor trip has not already been generated by any other reactor protective instrumentation, the engineered safety features automatic actuation signals initiate a reactor trip upon sensing any condition which initiates a safety injection. These trips are provided to protect the core in the event of a loss of coolant accident or a steam line break accident.

The means of actuating the engineered safety features trips are discussed in the engineered safety features actuation Chapter 12.3.

12.2.3.16 Turbine Trip

A turbine trip - reactor trip signal, Figure 12.2-14, is provided to protect the reactor coolant system from a thermal transient (over pressure or overtemperature). This trip occurs at a power of greater than 10% (P-7), or in plants with P-9 installed, at 50 percent. The signals used to sense that the turbine has tripped are:

1. four of four (4/4) turbine throttle valves fully closed or
2. two of three (2/3) low EHC trip header fluid pressure (800 psig - General Electric turbine) two of three (2/3) low auto-stop oil pressure (45 psig - Westinghouse turbine)

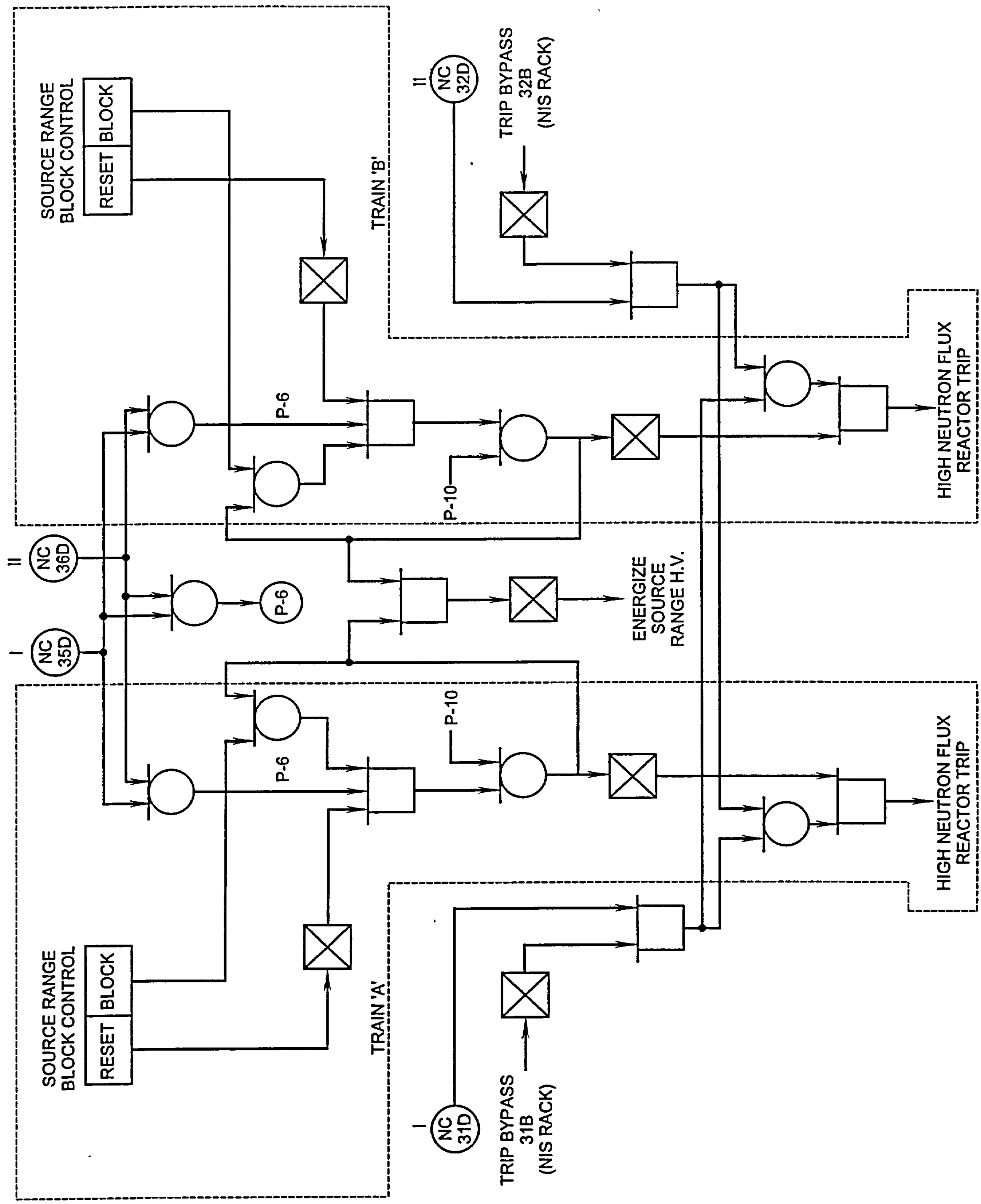


Figure 12.2-2 Source Range Reactor Trip Logic

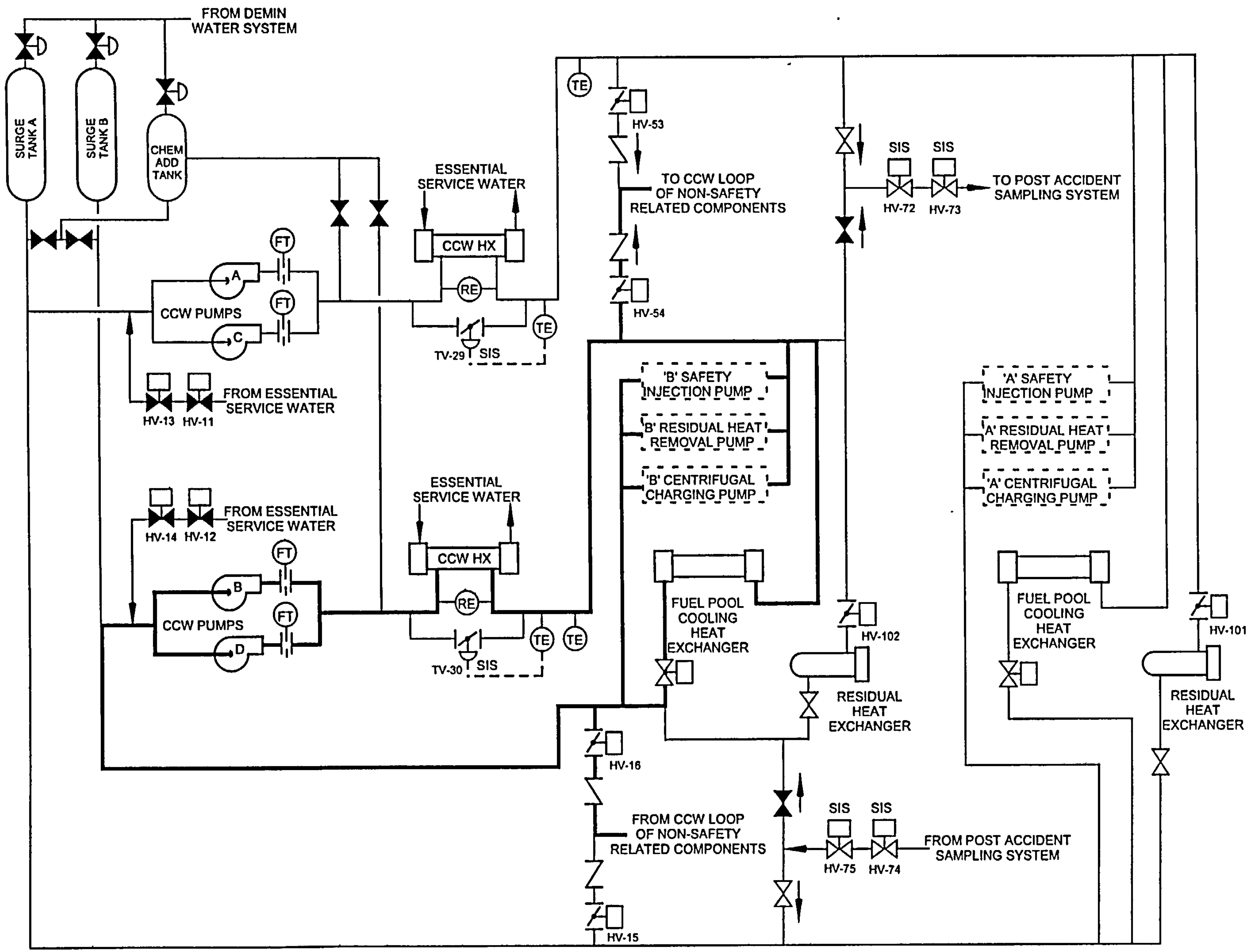


Figure 14.1-1 Component Cooling Water

C202-3

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

16.0 RADIATION MONITORING SYSTEM

Learning Objectives:

1. State the purposes of the radiation monitoring system.
2. List the two classes of radiation monitors and give four examples of each.
3. List four radiation monitors that provide automatic actions (other than alarms) and briefly describe the action provided.
4. List and briefly describe the two types of failed fuel monitors.
5. List the radiation monitors which identify the following:

   a. Primary to secondary leakage
   b. Primary to containment leakage

16.1 Introduction

The purposes of the radiation monitoring system (RMS) are as follows:

1. Continuously monitor radiation levels of various plant areas, processes and effluents.
2. Provide alarms and/or automatic actions if preset limits are exceeded.

The radiation monitoring system is divided into the following: process radiation monitoring (PMS), explained in Section 16.2.1, and area radiation monitoring (ARM), explained in Section 16.2.2.

16.2 System Description

16.2.1 Process Radiation Monitoring System

The PRM monitors the radiation level of various process liquid and gas streams that may serve as discharge routes for radioactive materials. These monitors are provided to indicate the radioactivity of the process stream and to alert operating personnel when operational limits are approached for the normal release of radioactive material to the environment.

On process streams that do not discharge to the environs, such as the component cooling water system (Section 14.1), process monitors are provided to indicate process stream malfunctions. This is accomplished by detecting the normal background radiation of the system and by alerting the operator with an annunciator if an accumulation of radioactive material occurs in the system. In addition to providing continuous indication and alarms, the PRM may provide various automatic functions, such as the closing of vent valves, discharge valves, etc.

If the activity level in the process stream reaches a predetermined setpoint, the system will perform its automatic function, which ensures that the discharge of radioactive material to the environs is limited. The PRM can monitor its process by one of two methods. These methods are called in-line monitors and off-line monitors.

IN-LINE monitor

An in-line monitor system has the detector probe directly immersed in the process stream. The advantage of this type of monitoring is that the detector probe will be provided a representative sample of the process and responds rapidly to activity changes. The disadvantages of this system are that if the process has a turbulent flow the detector probe must be protected by placing it in a well, which lowers the sensitivity of the probe, and if the probe fails, the system must either be secured or a means of bypassing flow around the probe must be provided (only for directly immersed probes).

OFF-LINE monitor

An off-line monitor system contains piping, valves, detector probes (usually two in parallel), and a motive force device, such as a pump or a fan. This system will take a suction on the process stream, pass the flow to the detector, and then return the sample to the process stream. The advantages of this system are that with lower flow rates, the detector probe can be directly immersed into the sample stream without a protection well, therefore increasing probe sensitivity, and if a detector fails, it can be isolated (by inlet and outlet valves), and the process stream is not affected.

The disadvantages of this system are that it may not be receiving a representative sample of the process stream and may not be as responsive to rapid changes of activity in the process. At the time of this writing there is no preferred method of process monitoring. Both types, IN-LINE and OFF-LINE monitors, are found throughout the industry.

16.2.2 Area Radiation Monitoring System

The ARM are located in selected areas of the plant, such as the Control Room, Containment Building, and various areas or rooms in the Auxiliary Building. The purposes of the area monitors are to give continuous indication of background radiation and to alert plant personnel of high radiation. The alarms associated with area radiation monitors include annunciators in the control room area and local alarms. The local alarms are at the radiation detectors and provide indication of high radiation both visually (flashing light) and audibly (horn or buzzer).

16.3 Component Description

16.3.1 Radiation Detectors

There are various types of detectors used in both the process and area radiation monitoring systems. Some of the most commonly used detectors will be explained in this section.

Geiger-Mueller Tube

The geiger-mueller (G-M) tube is a gas filled chamber with a center electrode as shown in Figure 16-1. The G-M tube operates by sensing an incident particle, such as a beta or gamma, interacting with the gas inside the chamber to produce a few ion pairs. As the ion pairs are accelerated towards the wall and electrode, they will produce more ions pairs until there are millions of ion pairs produced inside the chamber.

The affect of this mass production of ions is called avalanching and is the result of the high voltage potential between the chamber and the center electrode. When avalanching occurs, the millions of ions, both positive and negative, are collected on the chamber wall and center electrode. When this happens, a pulse is produced. The pulse is always the same size. Therefore, it is not possible to tell the type or energy of the incident particle from the pulse, but only that radiation is present.

This instrument will use a gas that is easily ionized, such as argon. However, when the positive ions are collected on the center electrode, secondary photons, in the form of ultraviolet light, are produced. These photons will then travel across the gas volume and interact with the walls of the chamber. This interaction produces electrons which starts the avalanche all over again. To prevent this undesired secondary avalanche, another gas is normally added to the chamber and mixed with the ionizing gas. This second gas is called a quenching gas and is normally a halogen, such as bromine or chlorine.

Once the avalanche occurs, the detector will be saturated with ions, and another incident particle entering the detector will not be seen. After the quenching takes place, the detector will be able to sense another incoming particle. Due to this time between avalanches and quenching, a G-M tube will only be useful in certain radiation fields. The problem with high radiation areas is that there are so many incident particles that the detector will stay saturated. When this occurs the output from the detector will go to zero, and the meter reading would be full downscale. To overcome this effect, the circuitry is designed so that the meter reading will read full scale if the detector becomes saturated.

Scintillation Detectors

The scintillation detector consists of a crystal, window, and a photo multiplier tube as shown in Figure 16-2.

The scintillation detector works on the principle that when a radioactive particle interacts with certain materials (crystal), light is produced. By measuring the light that is emitted, the energy and amount of the original radioactive particle can be determined. Scintillation detectors can accurately measure different types of radiation, such as alphas, betas, or gammas. This is accomplished by using different types of materials (crystals) for each type of radiation.

A scintillation detector is constructed such that it is sensitive to only one type of radiation, i.e., if beta and gamma radiation levels were to be measured in a process, both a beta scintillation and a gamma scintillation detector must be provided. The scintillation detector operates by a radioactive particle interacting with the crystal, which causes ionization of some of the atoms. These ionized atoms now have electrons in the excited state, but the excitation is not great enough for the electron to escape. Since these atoms are now in an excited state, they will radiate this excess energy in the form of photons (light rays).

The photons are transmitted from the sensing crystal to the photo multiplier tube via a quartz window. Quartz is used to transmit the light produced in the crystal because it will not distort the photons emitted from the crystal.

The photo multiplier tube consists of a photo cathode, dynodes, anode and outer chamber wall. The light produced by the crystal interacts with the photo cathode which then produces electrons. These electrons are then attracted to the first positively charged dynode. When an electron strikes the dynode several electrons will be produced (typically for each electron striking a dynode, two to four electrons will be produced).

The electrons produced by the dynode will then be directed to the next dynode for further multiplication. The result of this multiplication process is that generally about one million electrons are produced from each electron produced by the photo cathode. This large electron flow is then collected by the anode, and an electrical current is produced and measured by the circuitry. This circuitry can be setup so that the detectors output can be in counts per minute or as a dose rate in mrem or Rem per hour.

The scintillation detector is useful not only in detecting radiation, but also in laboratory work, since this detector can also measure the energy of the incident radiation. The energy can be measured because the pulse of electrons at the anode is proportional to the energy of the original incident radiation, i.e. the more energy the radioactive particle has, the more light that will be emitted from the crystal. This will in turn cause more electrons to be produced by the photo cathode, which after the electron multiplication, causes a larger pulse at the anode.

16.3.2 Plant Radiation Monitors

Containment Air Particulate Detector

The containment air particulate detector (Figure 16-4) is sufficiently sensitive for detection of reactor coolant leakage into the containment. This instrument is capable of detecting leakage rates of 5 cc/min. within minutes after the leak occurs.

Continuous air samples are taken from the containment atmosphere near the reactor containment fan cooler inlet, drawn outside the containment in a closed, sealed system, and monitored by a scintillation counter and movable filter paper detector assembly. The air sample is passed through a filter paper which collects 99% of all particulate matter greater than 0.3 microns in size. The constantly moving filter paper is viewed by the scintillation detector, which then transmits the activity level to the main control room.

The activity level is then indicated on a meter and on a recorder. The air sample, after passing through the detector, is returned to the containment. The detector is used principally to detect the following radioactive isotopes in the containment atmosphere: I-131, I-133, CS-134 and CS-137. Receipt of a high activity level in the containment will be annunciated in the control room. In addition to the annunciator, the following automatic actions will occur:

- The containment purge supply and exhaust dampers will close.
- The pressure and vacuum relief valves will close (if they are open).
- The containment fan cooler dampers shift to the accident mode (the fans, however, remain in fast speed).

There is a brief description of this system and the following Process Radiation Monitors in Table 16-1. The table lists the Process Monitor location, type of detector used, and the automatic actions provided by the monitor.

Containment Noble Gas Monitor

The containment gas monitor (Figure 16-4) is provided in order to supply the operator with information pertaining to the noble gas activity in the containment. This activity is due to neutron activation of the primary shield cooling air and from leaks in the reactor coolant system when operating with cladding defects in the fuel. Continuous samples are taken from the containment atmosphere. After the sample passes through the previously described air particulate monitor, it flows through a closed sealed system to the gas monitor assembly. The samples flow continuously to a fixed, shielded volume, where the activity is measured by a Geiger-Mueller tube or beta scintillation detector. The air sample is then returned to the containment. The activity level is sent to the main control room, where the level is indicated on a meter and on a recorder. The detector is used principally to detect the following noble gases: Kr-85, Ar-41, Xe-133 and Xe-135. Receipt of high activity will annunciate in the main control room. In addition to the annunciator, the following automatic actions will occur:

- The containment purge and exhaust dampers will close.
- The pressure and vacuum relief valves will close (if they are open).
- The containment fan cooler dampers shift to the accident mode (the fans, however, remain in fast speed).

The radio gas detector will supplement the information obtained from the air particulate monitor regarding the occurrence of leakage from the primary system.

Containment Purge Exhaust Monitor

This channel (Figure 16-4) monitors the effluent from the containment purge for gaseous activity, iodine, and particulate activity whenever the purge system is in operation. The system consists of three separate channels, one of which is a fixed filter air particulate monitor with a beta scintillation detector, the second is a Geiger-Mueller detector for monitoring gaseous activity, and the third is a spectrometer grade gamma scintillation detector for iodine monitoring.

Detector outputs are transmitted to the main control room where they provide indication on meters and recorders. High radioactivity during the containment purge operations will be annunciated in the control room. In addition to the alarm, the purge supply and exhaust dampers will automatically close.

Auxiliary Building Ventilation System Monitor

This channel (Figure 16-4) continuously monitors the ventilation system exhaust air from all the potentially contaminated equipment cubicles in the auxiliary building. This system uses one moving filter monitor for particulates and a fixed filter unit for iodine. The detector for particulates uses a moving filter paper and monitors this filter with a beta scintillation detector. For iodine monitoring, a spectrometer grade gamma scintillation detector is used.

The outputs from these detectors are transmitted to the main control room for indication on meters and recorders. High radioactivity from either detector will be annunciated in the main control room. Detection of high radioactivity from the iodine monitor will automatically realign the auxiliary building ventilation system so that the exhausts from the equipment cubicles will be routed through charcoal filter banks prior to exhausting to the atmosphere.

Plant Vent Stack Monitor

This channel (Figure 16-4) monitors the ventilation system air discharging from the auxiliary building ventilation system to the plant ventilation stack. The sample gas is returned to the suction of the auxiliary building exhaust fans. The channel utilizes four Geiger-Mueller tubes connected in parallel. The radioactivity is indicated by a meter and recorder located in the main control room. High radiation at this monitor will actuate an annunciator in the main control room. There are no automatic functions associated with this channel. This monitor is used principally to detect Kr-85, Ar-41, Xe-133, and Xe-135.

Control Room Intake Air Monitor

This channel continuously monitors the outside air intake to the control room. Two monitors, one for particulates and one for iodine, are provided. The particulate monitor uses moving filter paper and a beta scintillation detector, and the iodine monitor employs a fixed filter and gamma scintillation detector. The detector outputs are transmitted to the control room, where the radioactivity levels are indicated by meters and recorders. High radiation conditions are annunciated in the main control room. In addition to the annunciators, an alarm in either channel will cause the ventilation system air inlet to close, and makeup air, for maintaining a slightly pressurized control room, will be introduced from the turbine building.

Condenser Air Discharge Gas Monitor

This channel (Figure 16-4) receives a continuous air sample from the air ejector exhaust header, monitors it for gaseous radioactivity, and provides the plant operator with a rapid indication of a primary to secondary leak. The sample gas is returned to the gas effluent. This channel uses a G-M detector whose output is transmitted to the main control room for indication on meters and recorders. A high radiation condition will be annunciated in the main control room. There is no automatic function associated with this channel. This monitor is used principally to detect noble gases such as Kr-85, Xe-133, and Xe-135.

Steam Generator Blowdown Liquid Monitor

This channel (Figure 16-4) monitors the liquid phase of the secondary side of the steam generator for radioactivity, which would indicate a primary to secondary system leak, providing backup information to that of the condenser air ejector gas monitor. Samples from each of the four steam generator bottoms are mixed in a common header and the common sample is continuously monitored by a scintillation counter and holdup tank assembly. Upon indication of high radioactivity, each steam generator is individually sampled in order to determine which unit is leaking. The detector output is transmitted to the main control room where indication is provided by both a meter and a recorder. A high radiation condition will be annunciated in the control room. There are no automatic functions associated with this channel. This monitor is used principally to detect Co-60.

Component Cooling Water System Monitor

This channel continuously monitors the component cooling water system (Section 14.1) for activity which would be indicative of a leak from one of the components that this system is cooling. A gamma scintillation detector is used for this monitor, and its output is transmitted to the control room. The activity level is indicated on a meter and a recorder. A high radiation condition will be annunciated in the control room. After receiving this alarm, the operator will isolate the affected component to stop the radioactive in-leakage. In addition to the annunciator, the component cooling water surge tank vent valves will automatically close. The sensitivity range of this monitor is based on Co-60.

Service Water Effluent Discharge Monitor

This channel continuously monitors the service water system (Section 14.2) discharge to the ultimate heat sink. An increase in activity would be indicative of radioactive in-leakage to this system. A gamma scintillation detector is used for this monitor, and its output is transmitted to the control room. The activity level of this system is indicated on a meter and a recorder. A high radiation level in this system will be annunciated in the control room. There is no automatic function associated with this channel. The sensitivity of this monitor is based on Co-60.

Waste Disposal System Liquid Effluent Monitor

This channel (Figure 16-4) continuously monitors all waste disposal system liquid releases from the waste monitor tanks (Section 15.1).

A Geiger-Mueller detector monitors all effluent discharges. The signal from this monitor is transmitted to the control room for indication on a meter and a recorder. A high radiation level on this discharge line will annunciate in the control room. In addition to the annunciator, the discharge valve located on the discharge line will automatically close. The discharge valve is located far enough downstream of the monitor to allow for the closure of this valve prior to any unplanned radioactive release. A single monitor is provided on each discharge line and is considered adequate since the monitor tanks are sampled and analyzed prior to any allowable discharge flow. The release of liquid waste is under administrative control, and this monitor is provided to maintain surveillance over the release.

Gas Decay Tank Effluent Gas Monitor

This channel (Figure 16-4) monitors the radioactivity released through the plant vent, especially during the venting of the gas decay tanks (Section 15.3). The detector is either a G-M tube or a beta scintillation detector. The detector output is transmitted to the control room for indication on a meter and a recorder. A high radioactivity condition will be annunciated in the control room. In addition to the annunciator, the isolation valve on the gas decay tank's vent line will automatically close. This will terminate the release and will initiate operator action to establish and correct the cause of this alarm. This monitor principally is used to detect Kr-85, Xe-133, and Xe-135, and its sensitivity is based on Kr-85.

Area Radiation Monitoring System

This system consists of channels which monitor and indicate the radiation levels in various physical areas of the plant. Table 16-2 lists the most common locations of area monitors. The detectors most generally used for area monitors are G-M tubes, beta or gamma scintillation detectors, and in some cases, air particulate with fixed filter collectors may be used. The detector output is transmitted to the control room where the radioactivity level is indicated and recorded. If the radiation level in a particular area exceeds a preselected setpoint, an annunciator will alarm in the control room.

The area radiation monitoring system will normally supply indication and alarms, both in the control room and locally, and will provide no automatic functions. However, there is one channel which will normally provide an automatic function. If the fuel handling building pool area monitor (Figure 16-4) should alarm, it will cause the fuel handling ventilation exhaust to be routed from its normal exhaust to a special exhaust system, comprised of booster fans and activated charcoal filters.

16.4 System Interrelations

16.4.1 Gross Failed Fuel Detector

There are several different methods used to detect failed fuel, of which only two methods will be explained below.

The first method is to monitor the radiation level in the chemical and volume control system volume control tank room. In the event of a failure of a fuel assembly or fuel element, the radioactive noble gas inventory in the volume control tank will increase, this results in a higher radiation level inside the volume control tank room, thereby alerting the operator to the failure of a fuel assembly. The expected or predicted radiation levels in the volume control tank room are as follows:

- Reactor Shutdown ~ 1 millirem per hour
- Reactor Operating ~ 100 millirem per hour
- 1% Failed Fuel ~ 1000 rem per hour

The problem with this type of system is that with increasing reactor power, a phenomenon occurs called iodine spiking. This iodine spiking will cause the radiation level in the volume control tank room to increase to high levels, giving this system a false indication.

A second method used to detect failed fuel is with a neutron detector, as shown in Figure 16-3. This system continuously monitors the reactor coolant system via a sample line from the hot legs, through two containment isolation valves, a sample cooler, neutron detector, then through a flow control device where the sample is discharged to the chemical and volume control system letdown line.

The sample is supplied to the neutron detector (BF3 proportional counter) via two containment isolation valves. These valves will automatically isolate on a Phase B isolation signal. The detector is sampling for delayed neutrons from short lived fission products, namely bromine-87, iodine-137, and bromine-88.

The 40 second delay prior to the exit of containment is for N-16 gamma considerations, and the remaining 20 seconds is to ensure that the detector is sampling these particular fission products. The time delay is established with the length of the sample line and the flow control device. Normally, the flow rate through this system will be set at approximately one gallon per minute.

The detector is a calibrated BF3 proportional counter whose indication ranges from 10^1 counts per minute (cpm) to 10^6 cpm on a logarithmic scale. Generally, there are two alarms associated with this system. The high alarm is normally set at 2 x 10^4 cpm above a preselected level. When this alarm actuates, a chemistry sample is required of the reactor coolant system. This alarm is indicative of the possibility of some fuel damage.

The other alarm is the high-high alarm, which is set at 1 x 10^5 cpm above a preselected level. Upon the receipt of this alarm, an immediate sample of the reactor coolant system is required, and reactor power is to be reduced 25 percent. This alarm is an indication of excessive fuel defects or failures.

16.5 Summary

The radiation monitoring system is a system that will measure the radiation or activity levels in various process streams or areas. It will provide information to the operator in the control room with the use of indicating meters, recorders, and alarms, both audible and visual. The radiation monitoring system is comprised of two subsystems. These subsystems are known as process monitors and area monitors. Tables 16-1 and 16-2 list some of the processes or areas that are generally monitored. In addition to the detector locations, these tables will list the most commonly used detectors for that specific location and the automatic functions, if any, that this particular channel may provide. In addition to these monitors, the facilities will be provided with some type of system or component to detect a gross failure of the fuel.

Table 16-1
Process Radiation Monitors

Location	Detector Type	Automatic Action
a. Containment Air Particulate Detector	Gamma scint.	Isolates containment purge and exhaust if running. Isolates relief and vacuum lines. Shifts containment coolers to accident mode.
b. Containment Noble Gas Monitor	Beta scint.	Same as above
c. Purge Exhaust Monitor	APD, G-M tube, gamma scint.	Isolate containment purge supply and exhaust valves if running
d. Auxiliary Building Ventilation Monitor	Beta scint. Gamma scint.	Initiates auxiliary building isolation Diverts to gas treatment system
e. Plant Vent Stack Monitor	G-M tube	Alarm function only
f. Main Control Room Intake Air Particulate Monitor	Beta scint. Gamma scint.	Isolates main control room ventilation
g. Condenser Air Ejector Gas Monitor	G-M tube	Alarm function only
h. Steam Generator Blowdown Liquid Sample	Gamma scint.	Alarm function only
i. CCW - Downstream of Heat Exchanger	Gamma scint.	Closes CCW surge tank vent
j. Service Water Effluent Discharge	Gamma scint.	Alarm function only
k. Waste Disposal System Liquid Discharge to the Environment	Gamma scint. or G-M tube	Closes the effluent discharge to the environment
l. Gas Decay Tank Effluent Discharge Monitor	Beta scint. or G-M tube	Closes the effluent discharge to the environment

Blank

Table 16-2
Area Radiation Monitors

Location	Detector Type	Automatic Action
1. Main Control Room	G-M Tube	Alarm function only*
2. Containment a. Operating deck b. Seal table area c. Dome monitor	 G-M Tube or gamma scint. G-M Tube Ion Chamber	Alarm function only
3. Radio Chemistry Lab	G-M Tube	Alarm function only
4. Charging Pump Room	G-M Tube	Alarm function only
5. Drumming Station	G-M Tube or gamma scint.	Alarm function only
6. Sampling Room	G-M Tube	Alarm function only
7. Spent Fuel Building	G-M Tube or gamma scint.	Isolates auxiliary building exhaust to gas treatment system.
8. Dry Active Waste Storage Area	Air particulate beta scint.	Alarm function only
9. Gas Decay Tank Rooms	Air sample beta scint.	Alarm function only
10. Radwaste Evaporator Room	Air sample beta scint.	Alarm function only

*Some facilities may provide an automatic isolation of the normal control room ventilation system.

Blank

TABLE OF CONTENTS

LIST OF FIGURES

the coolant with the reinforced concrete walls of the cavity.

Fuel Transfer Canal

The canal is formed by two concrete shield walls, which extend upward to the same elevation as the refueling cavity. The floor of the fuel transfer canal and a portion of the refueling cavity is at a lower elevation than the reactor flange to provide the greater depth required for operation of the fuel transfer system upenders and the rod cluster control assembly change fixture. The fuel transfer tube enters the reactor containment and protrudes through the end of the fuel transfer canal. The fuel transfer tube is a 20 inch stainless steel pipe which connects the fuel transfer canal in the containment with the fuel canal in the fuel storage building.

Polar Crane

A large overhead crane has been provided to handle equipment inside containment. It is used to lift the reactor vessel head, and the reactor internals during the refueling sequence.

Manipulator Crane

The manipulator crane, Figure 17.1-11, is used to remove, replace and position fuel assemblies within the core. The manipulator consists of a rectilinear bridge and trolley with a vertical mast which extends into the refueling water. The controls for the following components, which are located on the manipulator crane, are shown on Figure 17.1-12. The bridge, which spans the reactor cavity, runs on rails set into the operating deck of the containment along the edge of the refueling cavity and transfer canal. The trolley runs on the bridge and positions the operators platform and mast assembly across the width of the refueling cavity.

Gripper Mast Assembly

The gripper assembly, Figure 17.1-13, is mounted on the bottom of the gripper tube. The gripper tube telescopes into and out of the mast. A hoist on the manipulator crane trolley raises and lowers this gripper tube. Movement of the gripper tube within the mast is guided by 7 sets of 3 roller bearings. The 3 rollers in each set are spaced evenly at 120 degree intervals and prevent the gripper tube from hanging up or swinging freely in the mast. The gripper assembly is air operated with air pressure needed to disengage the fingers. Raising and lowering of the gripper tube and gripper assembly is accomplished by the gripper tube hoist. The gripper tube is long enough so that the upper end is still contained in the mast when the gripper assembly contacts the fuel, yet short enough so that when the fuel is raised it is entirely contained within the mast to provide protection for the fuel assembly while being transported in the refueling cavity. Thus, fuel assembly protection and some additional shielding from the fuel assembly is provided. The mast is normally held stationary but may be rotated 300 degrees manually by retracting a position stop button and turning the outer mast with a turning bar.

Safety interlocks associated with manipulator crane travel and gripper tube hoist movement are designed to prevent damage to the fuel assembly being moved and the fuel remaining in the vessel. Figure 17.1-14 shows typical travel limits for the bridge and trolley positions. In an emergency, and for fine adjustments in position the bridge, trolley and hoist can be operated manually using hand wheels on the individual motor shafts.

Rod Cluster Control Assembly (RCCA) Change Fixture

The RCCA Change Fixture, Figure 17.1-15, is mounted on the transfer canal wall and is used in removing rod cluster control and spider mounted secondary source assemblies from spent fuel assemblies and inserting them into new or partially spent fuel assemblies. The fixture consists of two main components: a guide tube mounted to the wall for containing and guiding the withdrawn Rod Cluster Control (RCC) assemblies, and a mounted carriage for holding the fuel assemblies under the guide tube.

A rod cluster control assembly can be removed by the RCCA change fixture gripper and hoist. The rod cluster control assembly can be aligned with the other fuel assembly's guide tubes for insertion into the new fuel assembly. The RCCA change fixture gripper is raised and lowered in the guide tube by a cable driven from a hoist.

The RCCA change fixture gripper is pneumatically operated to latch and unlatch the RCCA assemblies. The wheel mounted carriage support is anchored to the floor of the refueling cavity. The carriage contains compartments for two fuel assemblies and one RCC element with each one capable of being positioned by a chain and cable assembly operated by a hand winch from the operating floor. This winch has a lock or shaft clamp on it to prevent movement. Two stationary stops have been attached to the extremes of the support frame. These stops will prevent the carriage from rolling off the ends of the tracks. Positioning stops are also provided on both the carriage and frame to locate each of the three carriage compartments directly below the guide tube.

Reactor Vessel Head Lifting Device

The reactor vessel head lifting device, Figure 17.1-16, consists of a welded and bolted structural steel frame with suitable rigging to enable the polar crane operator to lift the head and store it during refueling operations. The lifting device is permanently attached to the reactor vessel head. Attached to the head lifting device are the monorail and hoists for the reactor vessel stud tensioners.

Reactor Internals Lifting Device

The reactor internals lifting device, Figure 17.1-17, is a structural frame suspended from the polar crane. The frame is lowered onto the guide tube support plate of the internals, and is manually bolted to the support plate by three bolts. Bushings on the frame engage guide studs in the vessel flange to provide guidance during removal and replacement of the internals package. The reactor internals lifting device is used to lift the upper internals package as well as the lower reactor internals package.

Reactor Vessel Stud Tensioner

Stud tensioners, Figure 17.1-18, are employed to secure the head closure joint at every refueling. The stud tensioner is a hydraulically operated device that uses oil as the working fluid. Stud tensioners minimize the time required for the tensioning or unloading operations of the reactor vessel head bolts. Three tensioners are provided and are applied simultaneously to three studs located 120 degrees apart. A single hydraulic pumping unit operates the tensioners, which are hydraulically connected in series. The studs are tensioned to their operational load in two steps to prevent high stresses in the flange region and unequal loadings in the studs. Relief valves on each tensioner prevent overtensioning of the studs due to excessive pressure.

Special Refueling Tools

Control Rod Drive Shaft Unlatching Tool

The control rod drive shafts are unlatched and latched to the full length rod cluster assembly spiders using the control rod drive shaft unlatching tool, Figures 17.1-5 & 17.1-19. This tool is suspended from the auxiliary hoist on the manipulator crane and is operated from the bridge. The latching mechanism is pneumatically operated. All full length RCCA drive shafts are removed as a unit with the reactor vessel upper internals.

Burnable Poison Rod Assembly (BPRA) Handling Tool

The burnable poison rod assembly handling tool, Figure 17.1-5, is a long handled tool used in the spent fuel pool and fuel transfer canal to transfer irradiated burnable poison rod assemblies between two fuel assemblies or between a fuel assembly and a special insert temporarily placed on selected spent fuel assembly storage racks. The tool is suspended from the hoist on the spent fuel pool bridge. An operator standing on the bridge guides the tool and manually actuates the engagement and handling mechanisms.

Irradiation Sample Handling Tool

The irradiation sample handling tool, Figure 17.1-5, is a long handled tool used to remove the irradiation specimens from their holders located on the outer surface of either the thermal shield or the neutron pads inside the reactor vessel. The tool is suspended from the polar crane and operated from the manipulator crane bridge.

Rod Cluster Control Thimble Plug Tool

The rod cluster control thimble plug tool is a manually operated tool, Figure 17.1-5, and is used in the transfer canal to remove or insert the thimble plug in a fuel assembly. When transferring an RCCA from one fuel assembly to another, a thimble plug is inserted in the fuel assembly from which the RCCA was removed.

17.1.4 Fuel Transfer System

17.1.4.1 System Description

The fuel transfer system is located in the fuel transfer canal area of the containment and fuel storage building, and utilizes an underwater conveyor to move fuel between these two areas, Figure 17.1-10. The underwater air-motor driven conveyor system runs on tracks extending from the containment through the transfer tube and into the fuel storage building. The container section of the conveyor car receives a fuel assembly is then lowered by the upender to a horizontal position for passage through the tube. Following that operation it is raised to a vertical position by a second upender in the fuel transfer canal (in the spent fuel pool side). The spent fuel pool bridge hoist then removes the assembly from the conveyor and places it in storage. A blind flange supplied with containment penetration pressurization air is bolted on the transfer tube inside the containment to seal the reactor containment.

17.1.4.2 Component Description

Conveyor Car Assembly

The conveyor car assembly is made up of two parts: the conveyor car frame and the fuel assembly container. The conveyor car frame is built out of a long stainless steel pipe. Mounted on and welded to the pipe at eight locations are wheel assemblies. The wheels ride on tracks which extend from the containment to the fuel storage building. Located on the bottom of the car frame along its entire length is welded a roller chain. Two gears located on the drive frame assembly engage the chain and provide the driving force.

The fuel assembly container is pinioned at one end to the conveyor car and is capable of being rotated to the vertical position about this point. The container is provided with locating guides which mate with pins on the upender. It is through the pins that the upender attaches itself to the fuel assembly container. During normal operation the car travels without any difficulty; if the car were to become stuck in the tube or the transfer canal, the car can be retrieved by pulling on its attached emergency cable with the fuel storage building crane.

Drive Frame Assembly

The drive frame assembly consists of a two speed reversible air driven motor which turns two gears that are connected to the motor by a roller chain. The two gears engage the chain welded to the bottom of the conveyor car frame. By rotating the gears with the drive motor, the car is propelled along the track. The air to the drive motor is turned on and off through the operation of solenoid valves. The solenoid valves are controlled from the reactor side control panel.

Upenders (Lifting Mechanisms)

The upenders are made up of an "T" beam that pivots about a support which mates with guides located on the fuel assembly container support structure. The upender is raised and lowered with a cable driven by an electrically operated winch. A hand wheel has been provided to manually operate the winch.

Gate Valve

A wedge type gate valve is installed at the fuel storage building side of the fuel transfer tube to provide a means of isolating the fuel transfer tube. The valve is large enough to allow the conveyor car to pass freely.

Fuel Transfer Control System

The fuel transfer control system is located on two panels. The conveyor car and reactor side upender are operated from the panel located inside containment while the fuel storage building upender is controlled from the panel located in the fuel storage building. Various procedural requirements and an interlock system between the two control points provide adequate fuel, equipment, and personnel protection during the operation of the fuel transfer system.

17.1.5 Summary

The maximum design stress for the structures and for all parts involved in gripping, supporting, or hoisting the fuel assemblies is 1/5 of the ultimate strength of the material. This requirement applies to normal working load and emergency pullout loads, when specified, but not the earthquake loading. To resist safe shutdown earthquake forces, the equipment is designed to limit the stress for a combination of normal working forces plus safe shutdown earthquake forces.

The fuel handling building crane is provided to move new fuel and spent fuel casks in the fuel handling building. Movement of these loads by the fuel building crane is allowed in all areas of crane travel except directly over the spent fuel storage racks. These interlocks (mechanical stops) will help to eliminate the possibility of accidentally damaging the spent fuel.

The fuel transfer tube connecting the fuel transfer canal inside the containment and the fuel transfer canal in the fuel storage building is closed on the containment side by a blind flange at all times except during refueling operations. Two seals are located around the periphery of the blind flange with leak check provisions between them. The fuel transfer tube is isolated on the fuel

UNITED STATES
NUCLEAR REGULATORY COMMISSION
TECHNICAL TRAINING CENTER

WESTINGHOUSE TECHNOLOGY COURSE
(R-304P)

This manual is a text and reference document for the Westinghouse Technology Course. It should be used by you as a study guide during attendance at this course. This manual was compiled by staff members of the Technical Training Center in the Office of Human Resources.

The information in this manual was developed or compiled for NRC personnel in support of internal training and qualification programs. No assumptions should be made as to its applicability for any other purpose. Information or statements contained in this manual should not be interpreted as setting official NRC policy. This text is not specific to any particular nuclear power plant but it can be considered to be representative of the vendor design.

TABLE OF CONTENTS
Volume I

TABLE OF CONTENTS
Volume II

TABLE OF CONTENTS Volume II
(Continued)

Westinghouse Technology Systems Manual

Chapter 1

INTRODUCTION

Section

Westinghouse Technology Systems Manual

Section 1.1

<u>Reference Documents</u>

TABLE OF CONTENTS

LIST OF FIGURES

APPENDIX A

1.1 REFERENCE DOCUMENTS

Learning Objectives:

1. Identify the following reference documents giving a statement of their contents and/or functions:

   a. Code of Federal Regulations (CFR),
   b. Final Safety Analysis Report (FSAR),
   c. Regulatory Guides (Reg. Guides), and
   d. Technical Specifications (Tech. Specs.).

2. Define the following terms as stated in the reference documents:

   a. Design Basis,
   b. Reactor Coolant Pressure Boundary,
   c. Loss of Coolant Accident (LOCA),
   d. Single Failure, and
   e. Seismic Category 1.

1.1.1 Introduction

Many data sources were used in the preparation of this manual that provided specific information on the systems and operation of the typical Westinghouse facility. Included in these sources are the Final Safety Analysis Report (FSAR), Westinghouse topical reports (WCAP), Westinghouse system descriptions and training manuals from various Westinghouse facilities. Although these documents provide specific system information, there are also documents which provide information related to the minimum requirements for design, operation and testing of the systems and structures involved at a commercial nuclear facility. Documents included in this group are the Code of Federal Regulations (CFR), Technical Specifications, Regulatory Guides, and various industry standards. (Figure 1.1-1) The following sections provide a brief description of each of the major documents. Appendix A contains selected copies of sections of the reference documents described in this chapter for illustrative purposes.

1.1.2 Code of Federal Regulations

The Code of Federal Regulations (Figure 1.1-2) is a compilation of rules published in the Federal Register by the executive departments and agencies of the Federal Government. The Code of Federal Regulations is kept up to date by the individual issues of the Federal Register. These two publications are used together to determine the latest version of any given rule. Each year a new publication of the code is issued with changes incorporated.

The code is divided into 50 titles which represent broad areas subject to federal regulations. Each title is divided into chapters which usually bear the name of the issuing agency. Each chapter is divided into parts covering the specific regulatory areas.

Regulations associated with the Nuclear Regulatory Commission are contained in Title 10 -Energy, Chapter 1 - Nuclear Regulatory Commission, Parts 0-199. The regulations are cited using the title, part, section and paragraph designations. (Figure 1.1-3) For example, 10CFR50.34(b) refers to Title 10 of the Code of Federal Regulations, Part 50, Section 34, paragraph (b).

The following is a list and brief description of the parts of 10CFR that primarily apply to NRC licensed commercial nuclear reactors (Figures 1.1-4 and 4a):

- **Part 2** Policy and procedures related to issuing, amending, or revoking an operating license; enforcement actions; and public rule making.

- **Part 19** Requirements for disseminating information to nuclear plant workers concerning radiological working conditions, enforcement actions, etc. Rules of conduct for NRC inspections.

- **Part 20** Standards for protection against radiation.

- **Part 21** Reporting of defects and noncompliance

- **Part 50** Rules for license application, content of applications, facility design requirements, and reporting of events to the NRC.

  Appendix A - General Design Criteria
  Appendix B - Quality Assurance Criteria

- **Part 55** Rules and procedures for the licensing of reactor operators.

- **Part 71** Requirements for packaging, shipping and transportation of radioactive material.

- **Part 73** Requirements related to physical protection of the facility to protect against radiological sabotage and theft of special nuclear material.

- **Part 100** Reactor site criteria including population density, seismic and geologic evaluations.

  Appendix A -Seismic and Geologic Siting Criteria for Nuclear Power Plants

Included in all these parts are definitions of terms important to understanding the regulations. For example, the following terms are defined in 10CFR50 (Figure 1.1-5):

- "Design basis" means that information which identifies the specific functions to be performed by a structure, system, or component of a facility, and the specific values or ranges of values chosen for controlling parameters as reference bounds for design.

- "Reactor coolant system pressure boundary" means all those pressure containing components of water-cooled nuclear power reactors, such as pressure vessels, piping, pumps, and valves which are: (1) part of the reactor coolant system, or (2) connected to the reactor coolant system, up to and including (a) the outermost containment isolation valve in system piping which penetrates primary reactor containment, (b) the second of two valves normally closed during normal reactor operation in system piping which does not penetrate primary reactor containment, © the reactor coolant system safety and relief valves.

- "Loss of coolant accident" means those postulated accidents that result from the loss of reactor coolant at a rate in excess of the capability of the reactor coolant makeup system from breaks in the reactor coolant pressure boundary, up to and including a break equivalent in size to the double-ended rupture of the largest pipe of the reactor coolant system.

- "Single failure" means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component nor (2) a single failure of any passive component, results in a loss of the capability of the system to perform its safety functions.

- "Safe shutdown earthquake" is defined in 10CFR100 as that earthquake which is based upon an evaluation of the maximum earthquake potential considering the regional and local geology and seismology. The "safe shutdown earthquake" defines that earthquake which has commonly been referred to as the "design basis earthquake." It is that earthquake for which certain structures, systems, and components are designed to remain functional.

1.1.3 Final Safety Analysis Report(FSAR)

A Final Safety Analysis Report (FSAR) is submitted with each application for an operating license and includes a description of the facility, the design bases and limits on its operation, and a safety analysis of the structures, systems, and components of the facility. The function of the FSAR is to demonstrate the applicant's qualifications, capability, and planned controls to assure safe plant operation within the constraints of plant design , operating limitations and regulatory requirements. (Figure 1.1-6 and 7)

The requirement for having an FSAR and the minimum information required to be included is established in 10CFR50.34(b). (Attachment A, pages A-1 through A-3) For example, this regulation, in part, requires an evaluation and analysis of the emergency core cooling system (ECCS) cooling performance following postulated loss-of-coolant accidents to ensure that the requirements of 10CFR50.46 "ECCS Design Acceptance Criteria" are met. This analysis is included in FSAR Chapter 15 "Accident Analysis" along with evaluations to show safe plant response for other postulated normal and abnormal plant conditions. Other examples of information contained in the FSAR include the methods in which the licensee plans to meet the 10CFR50 Appendix B, Quality Assurance Criteria and the results of environmental and meteorology monitoring programs as they pertain to 10CFR100 requirements. The plant is required to maintain the FSAR current and submit the most up-to-date version to the NRC on a yearly basis (commonly referred to as the Updated FSAR or UFSAR).

1.1.4 Technical Specifications

The requirement for including Technical Specifications (Figure 1.1-8) as part of the license application is set forth in 10CFR50.36. (Attachment A, pages A-4 and A-5) The NRC approved Technical Specifications are issued to the facility as part of the operating license. (Attachment A, pages A-6 and A-7) The Technical Specifications establish minimum operating limits for the facility. Failure to comply with these limits may require the reduction of the allowable operating power level or in some cases even a complete shutdown and cooldown of the unit. (Attachment A, page A-8)

The basis for the operating limits established in Technical Specifications is the analyses and evaluations included in the FSAR. Operating within the established limits ensures that the assumptions made in the safety analyses are true for all operating conditions. Technical Specifications are organized into six sections. Each section is defined as follows:

1. The definition section contains defined terms used in the Technical Specifications including definitions of surveillance frequency notation and plant operational modes. The defined terms from the definitions section appear in capitalized type throughout the Technical Specifications.

2. Safety limits and limiting safety system settings are contained in the second section of Technical Specifications. Safety limits are limits upon important process variables which are found to be necessary to protect the integrity of the physical barriers which guard against the uncontrolled release of radioactivity to the environment. If any safety limit is exceeded the reactor shall be shutdown.

   Limiting safety system settings are settings for automatic protective devices related to those variables having significant safety functions. Where a limiting safety system setting is specified for a variable on which a safety limit has been placed, the setting will assure that automatic protective action will correct the abnormal situation before a safety limit is exceeded. Appropriate action for exceeding a limiting safety system setting may include shutting down the reactor.

3. Limiting conditions for operation (LCOs) are the lowest functional capability or performance levels of equipment required for safe operation of the facility. When an LCO is exceeded remedial action is required within a specified time frame.

4. Surveillance requirements are requirements relating to test, calibration, or inspection to assure that the necessary system or component quality is maintained.

5. Design features are those features of the facility such as materials of construction and structure arrangements which, if altered or modified, would have a significant effect on safety and are not covered in Sections 1-4.

6. Administrative controls are provisions related to organization and management, procedures, record keeping, review and audit, and reporting necessary to assure operation of the facility in a safe manner.

A bases section is included with the Technical Specifications as required by 10CFR50.36, and provides the reason(s) for each individual specification. (Attachment A, page A-9) The bases section is included with the Technical Specifications for information, but is not part of the Technical Specifications.

1.1.5 Codes and Standards

Due to the fact that the CFR is written in general terms, supplementary documentation is necessary to further define the requirements stated in the CFR. (Figure 1.1-9) Each FSAR contains a list of the specific codes and standards to which that particular licensee has committed to implement to fulfill regulatory obligations. The following sections describe three of the most used documents and include examples of each.

1.1.5.1 American National Standards Institute (ANSI) Standards

ANSI Standards cover a wide range of subjects. Certain ANSI standards were written to amplify the general design criteria of 10CFR 50 Appendix A. For example, ANSI Standard 18.2 defines the following design condition categories:

- Condition I - Normal Operation
- Condition II - Incidents of Moderate Frequency
- Condition III - Infrequent Incidents
- Condition IV - Limiting Faults

ANSI 18.2 defines each condition by the expected frequency of occurrence and its probability of deteriorating to a worse case condition. Design requirements for each condition are based on the amount of resulting core damage and radioactive release permitted. These design conditions and requirements are analyzed for each plant and the results are documented in the facility's FSAR (Attachment A, pages A-10 through A-13).

ANSI Standard 18.2a defines safety classes used to designate safety systems and components in accordance with their importance to nuclear safety. ANSI 18.2a defines a safety system as any system that is necessary to shutdown the reactor, cool the core, cool another safety system, or cool the reactor containment after an accident. In addition, any system that contains, controls, or reduces radioactivity released in an accident is a safety system. Safety Class 1 applies to components whose failure could cause a Condition III or Condition IV loss of reactor coolant accident. Safety Class 2 generally applies to reactor containment and RCS pressure boundary components not in Safety Class 1. Also included in Safety Class 2 are safety systems that remove heat from the reactor or reactor containment, circulate reactor coolant, or control radioactivity or hydrogen in containment. The last two safety classes, Safety Class 3 and Non-nuclear Safety Class, apply to other plant components related to safe plant operation or the potential uncontrolled release of radioactivity.

1.1.5.2 American Society of Mechanical Engineers (ASME) Code

ASME boiler and pressure vessel code is used to provide design criteria for fabrication, inspection, and construction of systems and vessels. The two most referred to sections with regard to nuclear plant systems are sections III and XI.

Section III. Rules for Construction of Nuclear Power Plant Components. The rules of this Section constitute requirements for the design, construction, stamping, and overpressure protection of nuclear power plant items such as vessels, concrete reactor vessels and concrete containments, storage tanks, piping systems, pumps, valves, core support structures, and components supports for use in, or containment of, portions of the nuclear power system of any power plant.

Section XI. Rules for Inservice Inspection of Nuclear Power Plant Components. The rules of this section constitute requirements for inservice inspection; non-destructive examination(NDE); and testing of pumps and valves in nuclear power plants. This section defines such things as required NDE of components or welds; allowable valve stroke times; and tolerances on pump flow, discharge pressure, and vibration. Requirements for the use of this section are contained in the plant technical specifications.

The ASME code also classifies components according to their use and importance to nuclear safety. Code Classes 1 - 3 correspond to ANSI 18.2a safety classes, with the exception of reactor containment components which are designated Code Class MC. These classifications specify design and quality assurance requirements.

The ASME code is constantly in a state of revision. To know which editions and addenda are required for a particular facility, 10CFR50.55a defines applicability according to issue date of the facility's construction permit. In addition, the FSAR contains information on the codes and standards that are followed during plant systems design and construction.

1.1.5.3 Institute of Electrical and Electronic Engineers (IEEE) Standards

IEEE standards are used in the design, operation, and testing of nuclear power plant electrical, and instrumentation components and systems. Some of the standards developed by IEEE are listed below.

(1) Criteria for Protection Systems for Nuclear Power Generating Stations
(2) Guide to the Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems.
(3) Guide for Qualification Testing of Nuclear Power Plant Protection Systems
(4) Guide for Qualification of Engineered Safety Feature Motors for Nuclear Fueled Generating Stations
(5) Guide for Qualification Testing of Electrical Cables Used in Nuclear Power Plants.
(6) Guide for Qualification Testing of Electrical Penetrations in Nuclear Plant Containments.

IEEE standards define as Class 1E, electrical equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment.

1.1.6 Regulatory Guides

NRC Regulatory Guides (Figure 1.1-10) were formerly called Safety Guides. They are not legal documents or requirements. However, they make available to the public methods acceptable to the NRC staff for complying with specific portions of 10CFR. In some cases a Regulatory Guide will endorse an industry standard in whole or part.

Applications for the use of Regulatory Guides are as follows:

(1) Amplification of the Code of Federal Regulations
(2) Endorse and/or supplement Industry Standards
(3) Provide guidance in ensuring specific regulatory requirements are met.

Each Regulatory Guide consists of four parts;

Introduction - References to applicable codes, standards, and Code of Federal Regulations associated with that particular subject.

Discussion - Information on the development of standards associated with the subject, and may address areas of disagreement, if any exists, concerning those standards.

Regulatory Position - Definitions acceptable to the NRC. Criteria, the basis for the criteria, and any additional information required to establish NRC's position on the particular subject,

Implementation - Defines the NRC staff use of the Regulatory Guide and any alternative methods acceptable for fulfilling the requirements discussed in the Regulatory Guide.

Regulatory Guide 1.29 "Seismic Design Classification" (Attachment A, pages A-14 through A-16) amplifies 10CFR50 and 10CFR100 requirements and provides the definition of Seismic Category 1. Seismic Category 1 refers to those plant structures, systems and components which are important to safety and are designed to remain functional in the event of a " Safe Shutdown Earthquake". Seismic Category 1 structures, systems, and components are necessary to assure: (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (3) the capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the guideline exposures of 10CFR100.

1.1.7 Summary

The interrelationships between the various reference documents can be illustrated using seismic design considerations as an example (Figure 1.1-11). General Design Criterion 2 of 10CFR50, Appendix A (Attachment A, page A-17) requires that certain systems be designed for protection against natural phenomena such as earthquakes. 10CFR100, Appendix A (Attachment A, page A-18) provides more specific requirements regarding the evaluations and analyses that must be done to ensure adequate seismic suitability of the site and design of the plant. These required evaluations and analyses are documented in the plant's FSAR. (Attachment A, page A-19) Individual Technical Specifications set forth the associated operating requirements to ensure that plant parameters are monitored and plant systems function as assumed in the FSAR, with the Bases section tying the particular specification back to the FSAR analyses. (Attachment A, pages A-20 and A-21) Any Regulatory Guides or industry standards that were used in the evaluation process may be referenced in the FSAR discussion and/or the Tech. Spec. Bases.

REFERENCE DOCUMENTS

CODE OF FEDERAL REGULATIONS

FINAL SAFETY ANALYSIS REPORT (FSAR)

TECHNICAL SPECIFICATIONS

OPERATING LICENSE

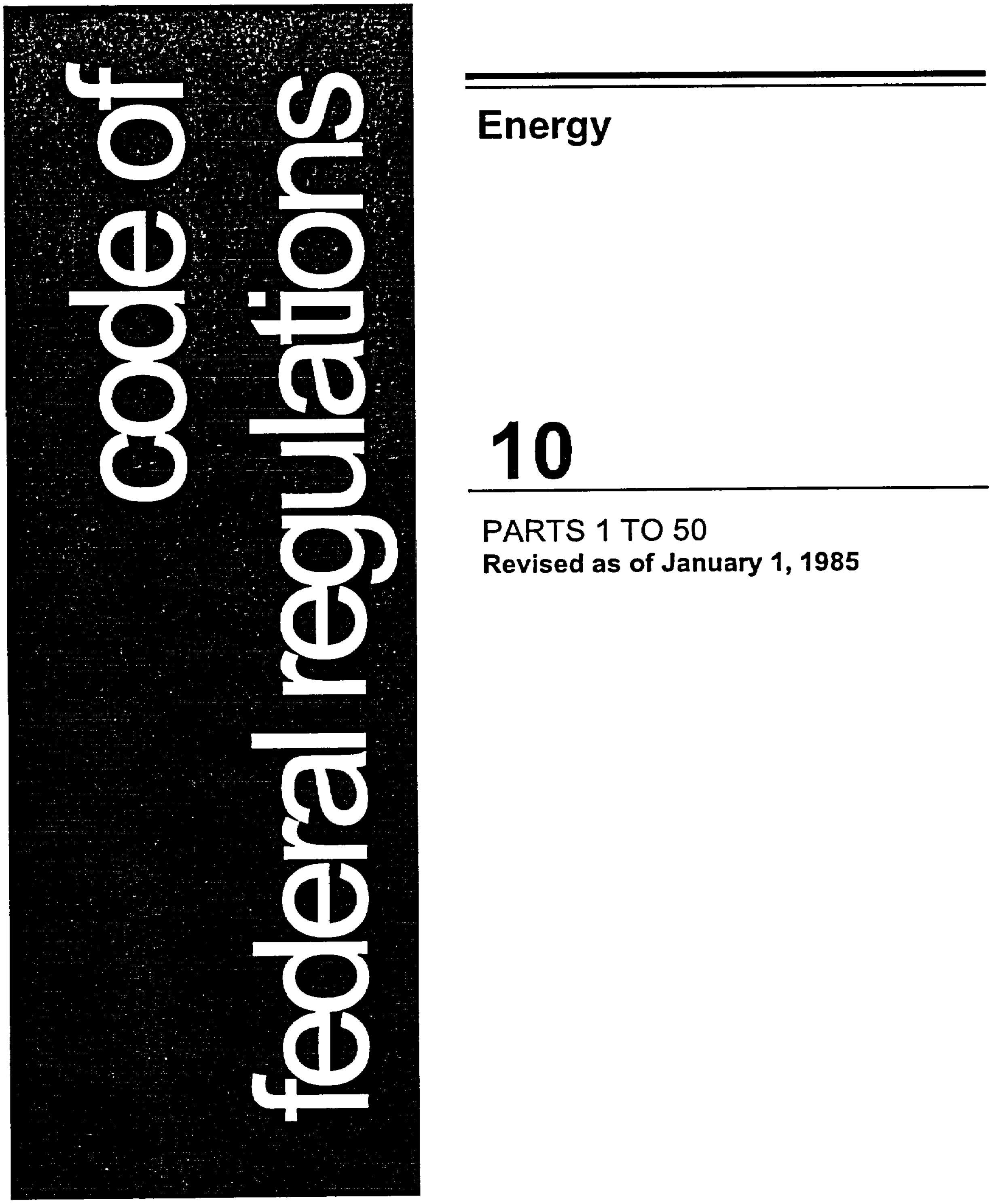
REGULATORY GUIDES

AMERICAN SOCIETY OF MECHANICAL ENGINEERS (ASME) BOILER AND PRESSURE VESSEL CODE

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE) STANDARDS

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI) STANDARDS

Figure 1.1-1 Reference Documents



code of federal regulations

Energy

10

PARTS 1 TO 50

Revised as of January 1, 1985

Figure 1.1- 2 Code of Federal Regulations

10 CFR 50.34(b)

Figure 1.1-3 Title, Chapter, Part

TITLE 10
CODE OF FEDERAL REGULATIONS

TABLE OF CONTENTS

Figure 1.1-4 Title 10, Table of Contents

10 CFR 50

DEFINITIONS

DESIGN BASIS

REACTOR COOLANT PRESSURE BOUNDARY

LOSS OF COOLANT ACCIDNET (LOOCA)

SINGLE FAILURE

Figure 1.1-5 10 CFR Definitions

10 CFR 50

DEFINITIONS

DESIGN BASIS

REACTOR COOLANT PRESSURE BOUNDARY

LOSS OF COOLANT ACCIDNET (LOOCA)

SINGLE FAILURE

Figure 1.1-6 10 CFR 50 Requirements

FSAR

Description and Safety Assessment of Site (10 CFR 100)

Descritpion of the Faciltiy Design and Design Bases
(10 CFR 50, Appendix A - ANSI 18.2A, Safety Classes)

Accident Analysis (10 CFR 50.46, ECCS Acceptance Criterial)
- Condition I - Normal Operation and Operational Transients
- Condition II - Faults of Moderate Frequency
- Condition III - Infrequent Faults
- Condition IV - Limiting Faults
  - (ANSI 18.2, Conditions for Design)

Technical Specification (10 CFR 50.36)

Description of Quality Assurance Program (10 CFR 50, Appendix B)

Other information (10 CFR 50.34(b))

Figure 1.1-7 Final Safety Analysis Reprott

10 CFR 50.36
TECHNICAL SPECIFICATIONS

Chapter 16 of FSAR

Validate assumptions made in FSAR analysis
Technical Specifications are Appendix A to the plants Operating License

The following must be included the Technical Specifications (10 CFR 50.36(c))

SAFETY LIMITS
LIMITING SAFETY SYSTEM SETTINGS
LIMITING CONDITIONS FOR OPERATION
SURVEILLANCE REQUIREMENTS
DESIGN FEATURES
ADMINISTRATIVE CONTROLS

Figure 1.1-8 Technical Specifications

10 CFR 50.55a
CODES AND STANDARDS

Incorporates by reference sections of the ASME Boiler & Pressure Vessel Code for Design, Construction, and Testing related to:

PRESSURE VESSELS
PIPING
PUMPS
VALVES
INSERVICE INSPECTION

Incorporates by reference IEEE Standard 279-1971 for Design and Testing of:

PROTECTION SYSTEMS

Figure 1.1-9 Codes and Standards

U.S. NUCLEAR REGULATORY COMMISSION
REGULATORY GUIDES

Amplifies the Code of Federal Regulations

Endorses/supplements Industry Standards

Provides guidance and/or additional information to the code

REGULATORY GUIDE contains the following:

A. Introduction
B. Discussion
C. Regulatory Position
D. Implementation

Figure 1.1-10 Regulatory Guides

10 CFR 100
REACTOR SITE CRITERIA

10 CFR 100, Appendix A, Seismic and Geologic Siting Criteria

SAFE SHUTDOWN EARTHQUAKE
OPERATING BASIS EARTHQUAKE

10 CFR 50, Appendix A, General Design Criterion 2
Design basis for protection against natural phenomena

Regulatory Guide 1.29 - Seismic Design Classification
Seismic Category I

Figure 1.1-11 10 CFR 100

ATTACHMENT A

§50.34 Contents of Applications; Technical Information.

(a)*Preliminary safety analysis report.* Each application for a construction permit shall include a preliminary safety analysis report. The minimum information[5] to be included shall consist of the following:

(1) A description and safety assessment of the site on which the facility is to be located, with appropriate attention to features affecting facility design. Special attention should be directed to the site evaluation factors identified in part 100 of this chapter. Such assessment shall contain an analysis and evaluation of the major structures, systems and components of the facility which bear significantly on the acceptability of the site under the site evaluation factors identified in part 100 of this chapter, assuming that the facility will be operated at the ultimate power level which is contemplated by the applicant. With respect to operation at the projected initial power level, the applicant is required to submit information prescribed in paragraphs (a)(2) through (8) of this section, as well as the information required by this paragraph, in support of the application for a construction permit.

(2) A summary description and discussion of the facility, with special attention to design and operating characteristics, unusual or novel design features, and principal safety considerations.

(3) The preliminary design of the facility including:

(i) The principal design criteria for the facility.[6] Appendix A, General Design Criteria for Nuclear Power Plants, establishes minimum requirements for the principal design criteria for water-cooled nuclear power plants similar in design and location to plants for which construction permits have previously been issued by the Commission and provides guidance to applicants

for construction permits in establishing principal design criteria for other types of nuclear power units;

(ii) The design bases and the relation of the design bases to the principal design criteria;

(iii) Information relative to materials of construction, general arrangement, and approximate dimensions, sufficient to provide reasonable assurance that the final design will conform to the design bases with adequate margin for safety.

(4) A preliminary analysis and evaluation of the design and performance of structures, systems, and components of the facility with the objective of assessing the risk to public health and safety resulting from operation of the facility and including determination of (i) the margins of safety during normal operations and transient conditions anticipated during the life of the facility, and (ii) the adequacy of structures, systems, and components provided for the prevention of accidents and the mitigation of the consequences of accidents. Analysis and evaluation of ECCS cooling performance following postulated loss-of-coolant accidents shall be performed in accordance with the requirements of §50.46 of this part for facilities for which construction permits may be issued after December 28, 1974.

(5) An identification and justification for the selection of those variables, conditions, or other items which are determined as the result of

---

[5]The applicant may provide information required by this paragraph in the form of a discussion, with specific references, of similarities to and differences from, facilities-ties of similar design for which applications have previously been filed with the Commission.

[6]General design criteria for chemical processing facilities are being developed.

preliminary safety analysis and evaluation to be probable subjects of technical specifications for the facility, with special attention given to those items which may significantly influence the final design: *Provided, however,* That this requirement is not applicable to an application for a construction permit filed prior to January 16,1969.

(6) A preliminary plan for the applicant's organization, training of personnel, and conduct of operations.

(7) A description of the quality assurance program to be applied to the design, fabrication, construction, and testing of the structures, systems, and components of the facility. Appendix B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," sets forth the requirements for quality assurance programs for nuclear power plants and fuel reprocessing plants. The description of the quality assurance program for a Nuclear power plant or a fuel reprocessing plant shall include a discussion of how the applicable requirements of appendix B will be satisfied.

(8) An identification of those structures, systems, or components of the facility, if any, which require research and development to confirm the adequacy of their design; and identification and description of the research and development program which will be conducted to resolve any safety questions associated with such structures, systems or components and a schedule of the research and development program showing that such safety questions will be resolved at or before the latest date stated in the application for completion of construction of the facility.

(9) The technical qualifications of the applicant to engage in the proposed activities in accordance with the regulations in this chapter.

(10) A discussion of the applicant's preliminary plans for coping with emergencies. Appendix E sets forth items which shall be included in these plans.

(11) On or after February 5, 1979, applicants who apply for construction permits for nuclear powerplants to be built on multiunit sites shall identify potential hazards to the structures systems and components important to safety of operating nuclear facilities from construction activities. A discussion shall also be included of any managerial and administrative controls that will be used during construction to assure the safety of the operating unit.

(b) *Final safety analysis report* . Each application for a license to operate a facility shall include a final safety analysis report. The final safety analysis report shall include information that describes the facility, presents the design bases and the limits on its operation, and presents a safety analysis of the structures, systems, and components and of the facility as a whole, and shall include the following:

(1) All current information, such as the results of environmental and meteorological monitoring programs, which has been developed since issuance of the construction permits relating to site evaluation factors identified in part 100 of this chapter.

(2) A description and analysis of the structures, systems, and components of the facility, with emphasis upon performance requirements, the bases, with technical justification therefor, upon which such requirements have been established, and the evaluations required to show that safety functions will be accomplished. The description shall be sufficient to permit understanding of the system designs and their relationship to safety evaluations.

(i) For nuclear reactors, such items as the reactor core, reactor coolant system, instrumentation and control systems, electrical systems, containment system, other engineered safety features, auxiliary and emergency systems, power conversion systems, radioactive waste handling systems, and fuel handling systems shall be discussed insofar as they are pertinent.

(ii) For facilities other than nuclear reactors, such items as the chemical physical, metallurgical, or nuclear process to be performed, instrumentation and control systems, ventilation and filter systems, electrical systems, auxiliary and emergency systems, and radioactive waste handling systems shall be discussed insofar as they are pertinent.

(3) The kinds and quantities of radioactive materials expected to be produced in the operation and the means for controlling and limiting radioactive effluents and radiation exposures within the limits set forth in part 20 of this chapter.

(4) A final analysis and evaluation of the design and performance of structures, systems, and components with the objective stated in paragraph (a)(4) of this section and taking into account any pertinent information developed since the submittal of the preliminary safety analysis report. Analysis and evaluation of ECCS cooling performance following postulated loss-of-coolant accidents shall be performed in accordance with the requirements of §50.46 for facilities for which a license to operate may be issued after December 28, 1974.

(5) A description and evaluation of the results of the applicant's programs, including research and development, if any, to demonstrate that any safety questions identified at the construction permit stage have been resolved.

(6)The following information concerning facility operation:

(i) The applicant's organizational structure, allocations or responsibilities and authorities, and personnel qualification requirements.

(ii) Managerial and administrative controls to be used to assure safe operation. Appendix B. "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," sets forth the requirements for such controls for nuclear power plants and fuel reprocessing plants. The information on the controls to be used for a nuclear power plant or a fuel reprocessing plant shall include a discussion of how the applicable requirements of appendix B will be satisfied.

(iii) Plans for preoperational testing and initial operations.

(iv) Plans for conduct of normal operations, including maintenance, surveillance, and periodic testing of structures, systems, components.

(v) Plans for coping with emergencies, which shall include the items specified in appendix E.

(vi) Proposed technical specifications prepared in accordance with the requirements of §50.36.

(vii) On or after February 5, 1979, applicants who apply for operating licenses for nuclear powerplants to be operated on multiunit sites shall include an evaluation of the potential hazards to the structures, systems, and components important to safety of operating units resulting from construction activities, as well as a description of the managerial and administrative controls to be used to provide assurance that the limiting conditions for operation are not exceeded as a result of construction activities at the multiunit sites.

(7) The technical qualifications of the applicant to engage in the proposed activities in accordance with the regulations in this chapter.

(8) A description and plans for implementation of an operator requalification program. The operator requalification program must as a minimum, meet the requirements for those programs contained in §55.59 of part 55 of this

chapter.

(9) A description of protection provided against pressurized thermal shock events, including projected values of the reference temperature for reactor vessel beltline materials as defined in §50.61 (b)(1) and (b)(2).

(c) *Physical security plan.* Each application for a license to operate a production or utilization facility shall include a physical security plan. The plan shall consist of two parts. Part I shall address vital equipment, vital areas, and isolation zones, and shall demonstrate how the applicant plans to comply with the requirements of part 73 (and part 11 of this chapter, if applicable, including the identification and description of jobs as required by §11.11(a), at the proposed facility). Part II shall list tests, inspections, and other means to be used to demonstrate compliance with such requirements, if applicable.

(d) *Safeguards contingency plan.* Each application for a license to operate a production or utilization facility that will be subject to §§73.50, 73.55, or §73.60 of this chapter must include a licensee safeguards contingency plan in accordance with the criteria set forth in appendix C to 10 CFR part 73. The safeguards contingency plan shall include plans for dealing with threats, thefts. and radiological sabotage, as defined in part 73 of this chapter, relating to the special nuclear material and nuclear facilities licensed under this chapter and in the applicant's possession and control. Each application for such a license shall include the first four categories of information contained in the applicant's safeguards contingency plan. (The first four categories of information as set forth in appendix C to 10 CFR part 73 are Background, Generic Planning, Base, and Responsibility Matrix. The fifth category of information, Procedures, does not have to be submitted for approval.)[7]

[7]A physical security plan that contains all the information required in both §73.55 and appendix C to part 73 satisfies the requirement for a contingency plan.

§50.36 Technical specifications.

(a) Each applicant for a license authorizing operation of a production or utilization facility shall include in his application proposed technical specifications in accordance with the requirements of this section. A summary statement of the bases or reasons for such specifications, other than those covering administrative controls, shall also be included in the application, but shall not become part of the technical specifications.

(b) Each license authorizing operation of a production or utilization facility of a type described in §50.21 or §50.22 will include technical specifications. The technical specifications will be derived from the analyses and evaluation included in the safety analysis report, and amendments thereto, submitted pursuant to §50.34. The Commission may include such additional technical specifications as the Commission finds appropriate.

(c) Technical specifications will include items in the following categories:

(1) *Safety limits, limiting safety system settings, and limiting control settings.* (i)(A) Safety limits for nuclear reactors are limits upon important process variables that are found to be necessary to reasonably protect the integrity of certain of the physical barriers that guard against the uncontrolled release of radioactivity. If any safety limit is exceeded, the reactor must be shut down. The licensee shall notify the Commission review the matter, and record the results of the review, including the cause of the condition and the basis for corrective action taken to preclude recurrence. Operation must not be resumed until authorized by the Commission. The licensee shall retain the record of the results of each review until the Commission terminates the license for the reactor, except for nuclear power reactors licensed under §50.21(b) or §50.22 of this part. For these reactors, the licensee shall notify the Commission as required by §50.72 and submit a Licensee Event Report to the Commission as required by §50.73. Licensees in these cases shall retain the records of the review for a period of three years following issuance of a Licensee Event Report.

(B) Safety limits for fuel reprocessing plants are those bounds within which the process variables must be maintained for adequate control of the operation and that must not be exceeded in order to protect the integrity of the physical system that is designed to guard against the uncontrolled release or radioactivity. If any safety limit for a fuel reprocessing plant is exceeded, corrective action must be taken as stated in the technical specification or the affected part of the process, or the entire process if required, must be shut down, unless this action would further reduce the margin of safety. The licensee shall notify the Commission, review the matter, and record the results of the review, including the cause of the condition and the basis for corrective action taken to preclude recurrence. If a portion of the process or the entire process has been shutdown, operation must not be resumed until authorized by the Commission. The licensee shall retain the record of the results of each review until the Commission terminates the license for the plant.

(ii)(A) Limiting safety system settings for nuclear reactors are settings for automatic protective devices related to those variables having significant safety functions. Where a limiting safety system setting is specified for a variable on which a safety limit has been placed, the setting must be so chosen that automatic protective action will correct the abnormal situation before a safety limit is exceeded. If, during operation, it is determined that the automatic safety system does not function as required, the licensee shall take appropriate action, which may include shutting down the reactor. The licensee shall notify the Commission, review the matter, and record the results of the review, including the cause of the condition and the basis for corrective action taken to preclude recurrence. The licensee shall retain the record of the results of each review until the Commission terminates the license for the reactor except for nuclear power reactors licensed under §50.21(b) or §50.22 of this part. For these reactors, the licensee shall notify the Commission as required by §50.72 and submit a Licensee Event Report to the Commission as required by §50.73. Licensees in these cases shall retain the records of the review for a period of three years following issuance of a Licensee Event Report.

(B) Limiting control settings for fuel reprocessing plants are settings for automatic alarm or protective devices related to those variables having significant safety functions. Where a limiting control setting is specified for a variable on which a safety limit has been placed, the setting must be 80 chosen that protective action, either automatic or manual, will correct the abnormal situation before a safety limit is exceeded. If, during operation, the automatic alarm or protective devices do not function as required, the licensee shall take appropriate action to maintain the variables within the limiting control-setting values and to repair promptly the automatic devices or to shut down the affected part of the process and, if required, to shut down the entire process for repair of automatic devices. The licensee shall notify the Commission, review the matter, and record the results of the review, including the cause of the condition and the basis for corrective action taken to preclude recurrence. The licensee shall retain the record of the results of each review until the Commission terminates the license for the plant.

(2) *Limiting conditions for operation.* Limiting conditions for operation are the lowest functional capability or performance levels of equipment required for safe operation of the facility. When a limiting condition for operation of a nuclear reactor is not met, the licensee shall shut down the reactor or follow any remedial action permitted by the technical specifications until the condition can be met. When a limiting condition for operation of any process step in the system of a fuel reprocessing plant is not met, the licensee shall shut down that part of the operation or follow any remedial action permitted by the technical specifications until the condition can be met. In the case of a nuclear reactor not licensed under §50.21(b) or §50.22 of this part or fuel reprocessing plant, the licensee shall notify the Commission, review the matter, and record the results of the review, including the cause of the condition and the basis for corrective action taken to preclude recurrence. The licensee shall retain the record of the results of each review until the Commission terminates the license for the nuclear reactor or the fuel reprocessing plant. In the case of nuclear power reactors licensed under §50.21(b) or §50.22, the licensee shall notify the Commission if required by §50.72 and shall submit a Licensee Event Report to the Commission as required by §50.73. In this case, licensees shall retain records associated with preparation of a Licensee Event Report for a period of three years following issuance of the report. For events which do not require a Licensee Event Report, the licensee shall retain each record as required by the technical specifications.

(3) *Surveillance requirements.* Surveillance requirements are requirements relating to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within

the safety limits, and that the limiting conditions of operation will be met.

(4) *Design features.* Design features to be included are those features of the facility such as materials of construction and geometric arrangements, which, if altered or modified, would have a significant effect on safety and are not covered in categories described in paragraphs (c) (1), (2), and (3) of this section.

(5) *Administrative controls.* Administrative controls are the provisions relating to organization and management, procedures, record keeping, review and audit, and reporting necessary to assure operation of the facility in a safe manner. Each licensee shall submit any reports to the Commission pursuant to approved technical specifications as specified in §50.4.

(6) *Initial notification.* Reports made to the Commission by licensees in response to the requirements of this section must be made as follows:

(i) Licensees that have an installed Emergency Notification System shall make the initial notification to the NRC Operations Center in accordance with §50.72 of this part.

(ii) All other licensees shall make the initial notification by telephone to the Administrator of the appropriate NRC Regional Office listed in appendix D, part 20, of this chapter.

(7) *Written Reports.* Licensees for nuclear power reactors licensed under §50.21(b) and § 50.22 of this part shall submit written reports to the Commission in accordance with §50.73 of this part for events described in paragraphs (c)(l) and (c)(2) of this section.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C 20555

DOCKET NO. 50-XXX

License No. DPR-ZZZ

TTC, UNIT 2

FACILITY OPERATING LICENSE

1. The Nuclear Regulatory Commission (the Commission) having found that:

A. The application for licenses filed by the ABC Corporation complies with the standards and requirements of the Atomic Energy Act, of 1954, as amended (the Act), and the Commission's Regulations set forth in 10 CFR Chapter I, and all required notifications to other agencies or bodies have been duly made;

B. Construction of the TTC, Unit 2 (the facility), has been substantially completed in conformity with Provisional Construction Permit No. CPPR-ZZZ and the application, as amended the provisions of the Act and the regulations of the Commission;

C. The facility will operate in conformity with the application, as amended. the provisions of the Act, and the regulations of the Commission;

D. There is reasonable assurance: (i) that the activities authorized by this operating license can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the regulations of the Commission set forth in 10 CFR Chapter I;

E. The ABC Corporation is technically and financially qualified to engage in the activities authorized by this operating license in accordance with the Commission's regulations set forth in 10 CFR Chapter I;

F. The ABC Corporation has satisfied the applicable provisions of 10 CFR Part 140, "Financial Protection Requirements and Indemnity Agreements", of the Commission's regulations;

G. The issuance of this license will not be inimical to the common defense and security or to the health and safety of the public;

(2) - (3) -----.

(4) Pursuant to the Act and 10 CFR Parts 30, 40 and 70, to receive, possess, and use in amounts as required any byproduct, source or special nuclear material without restriction to chemical or physical form, for sample analysis or instrument calibration or associated with radioactive apparatus or components; and

(5) Pursuant to the Act and 10 CFR Parts 30, 40 and 70, to possess, but not separate, such byproduct and special nuclear material as may be produced by the operation of the facility.

C. This license shall be deemed to contain and is subject to the conditions specified in the Commission's regulations set forth in 10 CFR Chapter I and subject to all applicable provisions of the Act and to the rules, regulations, and orders of the Commission now or hereafter in effect; and is subject to the additional conditions specified or incorporated below:

(1) Maximum Power Level

The TTC Unit 2 Power Plant is authorized to operate the facility at reactor core power levels not in excess of 3411 megawatts thermal.

(2) Technical Specifications

The Technical Specifications contained in Appendix A, as revised through Amendment No. 25 are hereby incorporated into the license. The licensee shall operate the facility in accordance with the Technical Specifications.

(3) Initial Test Program

The ABC Corporation shall conduct the post-fuel-loading initial test program (set forth in Section 14 of the TTC Unit 2 Plant Final Safety Analysis Report, as amended), without making any major modifications of this program unless modifications have been identified and have received prior NRC approval. Major modifications are defined as:

a. Elimination of any test identified in Section 14 of Final Safety Analysis Report as amended as being essential;
b. Modification of test objectives, methods or acceptance criteria for any test identified in Section 14 of Final Safety Analysis Report as amended as being essential;
c. Performance of any test at a power level different from there described; and ---.

Amendment 25

3/4.4.3 SAFETY AND RELIEF VALVES - OPERATING

SAFETY VALVES

LIMITING CONDITION FOR OPERATION

3.4.3.1 All pressurizer code safety valves shall be OPERABLE with a lift setting of 2485 psig (± 2%).

APPLICABILITY: MODES 1, 2, and 3.

ACTION:

a. With a pressurizer code safety valve inoperable, either restore the inoperable valve to OPERABLE status within 15 minutes or be in HOT SHUTDOWN within 12 hours.

b. In the event a safety valve fails or is found inoperable, a Special Report shall be prepared and submitted to the Commission pursuant to Specification 6.9.2 within 30 days. The report shall describe the circumstances surrounding the failure, including the cause, if known.

c. The provisions of Specification 3.0.4 may be suspended for one valve at a time for up to 18 hours for entry into and during operation in MODE 3 for the purpose of setting the pressurizer code safety valves under ambient (hot) conditions provided a preliminary cold setting was made prior to heatup.

SURVEILLANCE REQUIREMENTS

4.4.3 No additional Surveillance Requirements other than those required by Specification 4.0.5.

3/4.4.2 SAFETY VALVES and 3/4.4.3 SAFETY AND RELIEF VALVES

The pressurizer code safety valves operate to prevent the RCS from being pressurized above its Safety Limit of 2735 psig. Each safety valve is designed to relieve 420,000 lbs per hour of saturated steam at 110% of the valve's setpoint. The relief capacity of a single safety valve is adequate to relieve any overpressure condition which could occur during shutdown. In the event that no safety valves are OPERABLE, an operating RHR loop, connected to the RCS, provides overpressure relief capability and will prevent RCS overpressurization.

During operation, all pressurizer code safety valves must be OPERABLE to prevent the RCS from being pressurized above its safety limit of 2735 psig. The combine relief capacity of all these valves is greater than the maximum surge rate resulting from a complete loss of load assuming no reactor trip until the first Reactor Protective System trip setpoint is reached (i.e., no credit is taken for a direct reactor trip on the loss of load) and also assuming no operation of the power-operated relief valves (PORVs) or steam dump valves.

Demonstration of the safety valves' lift settings will occur only during shutdown and will be performed in accordance with the provisions of Section XI of the ASME Boiler and Pressure Vessel Code.

The OPERABILITY of the PORVs and block valves is determined on the basis of their being capable of performing the following functions:

a. Manual control of PORVs to control reactor coolant system pressure. This is a function that is used for the steam generator tube rupture accident and for Plant shutdown under abnormal conditions.

b. Maintaining the integrity of the reactor coolant pressure boundary. This is a function that is related to controlling identified leakage and ensuring the ability to detect unidentified reactor coolant pressure boundary leakage.

c. Manual control of the block valve to: (1) unblock an isolated PORV to allow it to be used for manual control of reactor coolant system pressure, and (2) isolate a PORV with excessive seat leakage.

d. Manual control of a block valve to isolate a stuck-open PORV.

The PORVs are also used to provide automatic pressure control in order to reduce challenges to the code safety valves for overpressurization events. (The PORVs are not credited in the over-pressure accident analysis as noted above.)

Surveillance Requirements provide the assurance that the PORVs and block valves can perform their functions. Specification 4.4.3.2.1 addresses PORVs and 4.4.3.2.2 the block valves. The block valves are exempt from the surveillance requirements to cycle the valves when they have been closed to comply with ACTION Requirements b. or c. This precludes the need to cycle the valves with full system differential pressure or when maintenance is being performed to restore an inoperable PORV to OPERABLE status.

15.0 ACCIDENT ANALYSES

15.1 CONDITION I — NORMAL OPERATION & OPERATIONAL TRANSIENTS

Condition I occurrences are those which are expected frequently or regularly in the course of power operations, refueling, maintenance, or maneuvering of the plant. As such, Condition I occurrences are accommodated with margin between any plant parameter and the value of that parameter which would require either automatic or manual protective action. In as much as Condition I occurrences occur frequently or regularly, they must be considered from the point of view of affecting the consequences of fault conditions (Conditions II, III, IV). In this regard, analysis of each fault condition described is generally based on a conservative set of initial conditions corresponding to the most adverse set of conditions which can occur during Condition I operation. A typical list of BWR Condition I transients include the following:

1. Steady state and shutdown operation

    a. Power operation (~ 15 to 100 percent of full power)
    b. Start up or standby (critical, 0 to 15 percent of full power)
    c. Hot shutdown (subcritical, Residual Heat Removal System isolated)
    d. Cold shutdown (subcritical, Residual Heat Removal System in operation)
    e. Refueling

2. Operations with permissible deviations

    Various deviations which may occur during continued operation as permitted by the plant Technical Specifications must be considered in conjunction with other operational modes. These include:

    a. Operation with components or systems out of service
    b. Equipment test and surveillance
    c. Leakage from fuel with cladding defects
    d. Activity in the reactor coolant
        i. Fission Products
        ii. Corrosion products

3. Operational transients

    a. Plant heatup and cooldown (up to $100^{0}F$/hour) for the reactor Coolant System
    b. Step load changes
    c. Ramp load changes

15.2 CONDITION II - FAULTS OF MODERATE FREQUENCY

These faults at worst result in the reactor shutdown with the plant being capable of returning to operation. By definition, these faults (or events) do not propagate to cause a more serious fault, i.e. Condition III or IV category. In addition, Condition II events are not expected to result in fuel rod failures or Reactor Coolant System overpressurization. A typical list of BWR Condition II faults include the following:

1. Scram - manual or inadvertant
2. Continuous control rod withdrawal error
3. Out of sequence control rod movement
4. Recirculation pump(s) trip
5. Inadvertant start-up of an inactive reactor coolant loop
6. Recirculation flow control system failure
7. MSIV closure - single or full
8. Inadvertant operation of one SRV - open/closing, stuck open
9. Minor leak from the reactor pressure boundary
10. EHC system failure - excessive cooldown/depressurization
11. Main turbine trip with BPV system available
12. Main generator load rejection with BPV system available
13. Loss of normal feedwater
14. Malfunction of the feedwater control system
15. Loss of feedwater heating
16. Loss of plant air systems
17. Loss of condenser vacuum
18. Loss of shutdown cooling
19. Loss of normal in-plant ac power
20. Loss of offsite ac power
21. Inadvertant startup of HPCS/HPCI at power

15.3 CONDITION III - INFREQUENT FAULTS

By definition Condition III occurrences are faults which may occur very infrequently during the life of the plant. They will be accommodated with the failure of only a small fraction of the fuel rods although sufficient fuel damage might occur to preclude resumption of the operation for a considerable outage time. The release of radioactivity will not be sufficient to interrupt or restrict public use of those areas beyond the exclusion radius. A Condition III fault will not, by itself, generate a Condition IV fault or result in a consequential loss of function of the Reactor Coolant System or containment barriers. A typical list of BWR Condition III faults include the following:

1. Loss of reactor coolant, from small ruptured pipes or from cracks in large pipes, which actuates emergency core cooling
2. Inadvertant loading and operation of a fuel assembly in an improper position
3. Unexplained reactivity addition
4. Main generator trip (load rejection) with BPV system failure
5. Main turbine trip with BPV system failure
6. One recirculation pump shaft seizure.
7. One recirculation pump shaft break.

15.4 CONDITION IV - LIMITING FAULTS

Condition IV occurrences are faults which are not expected to take place, but are postulated because their consequences would include the potential or the release of significant amounts of radioactive material. These are the most drastic which must be designed against and thus represent limiting design cases. Condition IV faults are not to cause a fission product release to the environment resulting in an undue risk to the public health and safety in excess of guideline values of 10CFR Part 100. A single Condition IV fault is not to cause a consequential loss of required functions of systems needed to cope with the fault including those of the Emergency Core Cooling System (ECCS) and the containment. A typical list of BWR Condition IV faults include the following:

1. Major rupture of piping containing reactor coolant up to and including double-ended rupture of the largest pipe in the reactor coolant pressure boundary located inside the primary containment (loss of coolant accident).
2. Small to large steam and liquid piping breaks outside the primary containment.
4. Control rod drop accident.
5. Control rod drive housing rupture.
6. Fuel handling accident.

The analysis of thyroid and whole body doses, resulting from Safety Analysis Report. The fission product inventories which form a basis for these calculations are presented in Chapter 11 and Section 15.1. The Safety Analysis Report also includes the discussion of systems interdependency contributing to limiting fission product leakages from the containment following a Condition IV occurrence.

U.S. NUCLEAR REGULATORY COMMISSION

Revision 3
September 1978

REGULATORY GUIDE

OFFICE OF STANDARDS DEVELOPMENT

REGULATORY GUIDE 1.29
SEISMIC DESIGN CLASSIFICATION

A. INTRODUCTION

General Design Criterion 2, "Design Basis for Protection Against Natural Phenomena," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," requires that nuclear power plant structures, systems, and components important to safety be designed to withstand the effects of earthquakes without loss of capability to perform their safety functions.

Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 establishes quality assurance requirements for the design, construction, and operation of nuclear power plant structures, systems, and components that prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. The pertinent requirements of Appendix B apply to all activities affecting the safety-related functions of those structures, systems, and components.

Appendix A, "Seismic and Geologic Siting Criteria for Nuclear Power Plants," to 10 CFR Part 100, 'Reactor Site Criteria," requires that all nuclear power plants be designed so that, if the Safe Shutdown Earthquake (SSE) occurs, certain structures, systems, and components remain functional. These plant features are those necessary to ensure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (3) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the guideline exposures of 10 CFR Part 100.

This guide describes a method acceptable to the NRC for identifying and classifying those features of light--water-cooled nuclear power plants that should be designed to withstand the effects of the SSE. The Advisory staff Committee on Reactor Safeguards has been consulted regarding this guide and has concurred in the regulatory position.

B. DISCUSSION

After reviewing a number of applications for construction permits and operating licenses for boiling and pressurized water nuclear power plants, the NRC staff has developed a seismic design classification system for identifying those lplant feature that should be designed to withstand the effects of the SSE. Those structures, systems, and components that should be designed to remain functional if the SSE occurs have been designated as Seismic Category I.

C. REGULATORY POSITION

1. The following structures, systems, and components of a nuclear power plant, including their foundations and supports, are designated as Seismic Category I and should be designed to withstand the effects of the SSE and remain functional. The pertinent quality assurance requirements of Appendix B to 10 CFR Part 50 should be applied to all activities affecting the safety-related functions of these structures, systems, and components.

a. The reactor coolant pressure boundary.

b. The reactor core and reactor vessel internals.

c. Systems[1] or portions of systems that are required for (1) emergency core cooling, (2) postaccident containment heat removal, or (3) postaccident containment atmosphere cleanup (e.g., hydrogen removal system).

d. Systems[1] or portions of systems that are required for (1) reactor shutdown, (2) residual heat removal, or (3) cooling the spent fuel storage pool.

e. Those portions of the steam systems of boiling water reactors extending from the outermost containment solation valve up to but not including the turbine stop valve, and connected piping of 2 1/2 inches or larger nominal pipe size up to and including the first valve that is either normally closed or capable of automatic closure during all modes of normal reactor operation. The turbine stop valve should be designed to withstand the SSE and maintain its integrity.

f. Those portions of the steam and feedwater systems of pressurized water reactors extending from and including the secondary side of steam generators up to and including the outermost containment isolation valves, and connected piping of 2 1/2 inches or larger nominal pipe size up to and including the first valve (including a safety or relief valve) that is either normally closed or capable of automatic closure during all modes of normal reactor operation.

g. Cooling water, component cooling, and auxiliary feedwater systems[1] or portions of these systems, including the intake structures, that are required for (1) emergency core cooling, (2) postaccident containment heat removal, ()3) postaccident containment atmosphere cleanup, (4) residual heat removal from the reactor, or (5) cooling the spent fuel storage pool.

h. Cooling water and seal water systems[1] or portions of these systems that are required for functioning of reactor coolant system components important to safety, such as reactor coolant pumps.

i. Systems[1] or portions of systems that are required to supply fuel for emergency equipment.

j. All electric and mechanical devices and circuitry between the process and the input terminals of the actuator systems involved in generating signals that initiate protective action.

k. Systems[1] or portions of systems that are required for (1) monitoring of systems important to safety and (2) actuation of systems important to safety.

l. The spent fuel storage pool structure, including the fuel racks.

m. The reactivity control systems, e.g., control rods, control rod drives and boron injection system.

n. The control room, including its associated equipment and all equipment needed to maintain the control room within safe habitability limits for personnel and safe environmental limits for vital equipment.

o. Primary and secondary reactor containment.

p. Systems,[1] other than radioactive waste management systems,[2] not covered by items 1.a through 1.o above that contain or may contain radioactive material and whose postulated failure would result in conservatively calculated potential offsite doses (using meteorology as recommended in Regulatory Guide 1.3, "Assumptions Used for Evaluating the Potential Radiological Consequences of a Loss of Coolant Accident for Boiling Water Reactors,": and Regulatory Guide 1.4, "Assumptions Used for Evaluating the Potential Radiological Consequences of a Loss of Coolant Accident for Pressurized Water Reactors") that are more than 0.5 rem to the whole body or its equivalent to any part of the body.

q. The Class 1E electric systems, including the auxiliary systems for the onsite electric power supplies, that provide the emergency electric power needed for functioning of plant features included in items 1.a through 1.p above.

2. Those portions of structures, systems, or components whose continued function is not required but whose failure could reduce the functioning of any plant feature included in items 1.a through 1.q above to an unacceptable safety level or could result in incapacitating injury to occupants of the control room should be designed and constructed so that the SSE would not cause such failure.[3]

3. Seismic Category I design requirements should extend to the first seismic restraint beyond the defined boundaries. Those portions of structures, systems, or components that form interfaces between Seismic Category I and non-Seismic Category I features should be designed to Seismic Category I requirements.

4. The pertinent quality assurance requirements of Appendix B to 10 CFR Part 50 should be applied to all activities affecting the safety-related functions of those portions of structures, systems, and components covered under Regulatory Positions 2 and 3 above.

D. IMPLEMENTATION

The purpose of this section is to provide information to applicants regarding the NRC staff's plans for using this regulatory guide.

This guide reflects current NRC staff practice. Therefore, except in those cases in which the applicant proposes and acceptable alternative method for complying with specified portions of the Commission's regulations, the method described herein is being and will continue to be used in the evaluation of submittals for operating license or construction permit applications until this guide is revised as a result of suggestions from the public or additional staff review.

---

[1] The system boundary includes those portions of the system required to accomplish the specified safety function and connected piping up to and including the first valve (including a safety or relief valve) that is either normally closed or capable of automatic closure when the safety function is rsequired.

[2] Specific guidance on seismic requirements for radioactive waste management systems is under development.

[3] Wherever practical, structures and equipment whose failure could possible cause such injuries should be relocated or separated to the extent required to eliminate this possibility.

DEFINITIONS AND EXPLANATIONS

Nuclear power unit. A nuclear power unit means a nuclear power reactor and associated equipment necessary for electric power generation and includes those structures, systems, and components required to provide reasonable assurance the facility can be operated without undue risk to the health and safety of the public.

Loss of coolant accidents. Loss of coolant accidents mean those postulated accidents that result from the loss of reactor coolant at a rate in excess of the capability of the reactor coolant makeup system from breaks in the reactor coolant pressure boundary up to and including a break equivalent in size to the double-ended rupture of the largest pipe of the reactor coolant system.[1]

Single failure. A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety, functions.[2]

Anticipated operational occurrences. Anticipated operational occurrences mean those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit and include but are not limited to loss of power to all recirculation pumps, tripping of the turbine generator set, isolation of the main condenser, and loss of all offsite power.

CRITERIA

I. *Overall Requirements*

Criterion 1—Quality standards and records. Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems. and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit;

[1] Further details relating to the type, size, and orientation of postulated breaks in specific components of the reactor coolant pressure boundary are under development.

[2] Single failures of passive components in electric systems should be assumed in designing against a single failure. The conditions under which a single failure of a passive component in a fluid system should be considered in designing the system against a single failure are under development.

Criterion 2—Design bases for protection against natural phenomena. Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions. The design bases for these structures, systems, and components shall reflect (1) Appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena and (3) the importance of the safety functions to be performed.

Criterion 3—Fire protection. Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions.

APPENDIX A TO PART 100 SEISMIC AND GEOLOGIC SITING CRITERIA FOR NUCLEAR POWER PLANTS

I.PURPOSE

General Design Criterion 2 of Appendix A to part 50 of this chapter requires that nuclear power plant structures, systems, and components important to safety be designed to withstand the effects of natural phenomena such as earthquakes. tornadoes. hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions. It is the purpose of these criteria to set forth the principal seismic and geologic considerations which guide the Commission in its evaluation of the suitability of proposed sites for nuclear power plants and the suitability of the plant design bases established in consideration of the seismic and geologic characteristics of the proposed sites.

These criteria are based on the limited geophysical and geological information available to date concerning faults and earthquake occurrence and effect. They will be revised as necessary when more complete information becomes available.

II. SCOPE

These criteria, which apply to nuclear power plants, describe the nature of the investigations required to obtain the geologic and seismic data necessary to determine site suitability and provide reasonable assurance that a nuclear power plant can be constructed and operated at a proposed site without undue risk to the health and safety of the public. They describe procedures for determining the quantitative vibratory ground motion design basis at a site due to earth quakes and describe information needed to determine whether and to what extent a nuclear power plant need be designed to withstand the effects of surface faulting. Other geologic and seismic factors required to be taken into account in the siting and design of nuclear power plants are identified.

The investigations described in this appendix are within the scope of investigations permitted by §50.10(c)(1) of this chapter.

Each applicant for a construction permit shall investigate all seismic and geologic factors that may affect the design and operation of the proposed nuclear power plant irrespective of whether such factors are explicitly included in these criteria. Additional investigations and/or more conservative determinations than those included in these criteria may be required for sites located in areas having complex geology or in areas of high seismicity. If an applicant believes that the particular seismology and geology of a site indicate that some of these criteria, or portions; thereof, need not be satisfied, the specific sections of these criteria should be identified in the license application, and supporting data to justify clearly such departures; should be presented.

These criteria do not address investigations of volcanic phenomena required for sites located in areas of volcanic activity. Investigations of the volcanic aspects of such sites will be determined on a case-by-case basis.

III. DEFINITIONS

As used in these criteria:

(a) The *magnitude* of an earthquake is a measure of the size of an earthquake and is related to the energy released in the form of seismic waves. *Magnitude* means the numerical value on a Richter scale.

(b) The *intensity* of an earthquake is a measure of its effects on man, on man-built structures, and on the earth's surface at a particular location. Intensity means the numerical value on the Modified Mercalli scale.

(c) The *Safe shutdown Earthquake* [1] is that earthquake which based upon an evaluation of the maximum earthquake potential considering the regional and local geology and seismology and specific characteristics of local subsurface material. It is that earthquake which produces the maximum vibratory ground motion for which certain structures, systems, and components are designed to remain functional.

---

[1]The *Safe Shutdown Earthquake* defines that earthquake which has commonly been referred to as the Design Basis Earthquake.

3.2 CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS

3.2.1 Seismic Qualifications

The TTC Unit 2 Nuclear Plant structures, systems, and components important to safety have been designed to remain functional in the event of a Safe Shutdown Earthquake (SSE). These structures, systems, and components, designated as Category I, are those necessary to assure:

1. The integrity of the reactor coolant pressure boundary.

2. The capability to shut down the reactor and maintain it in a safe shutdown condition.

3. The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the guideline exposures of 10 CFR Part 100.

Moreover, those safety-related structures, systems, and components necessary to assure the above requirements, have been designed to stress limits that are well within the material yield limits to withstand the loading effects of vibratory motion of at least 50 percent of the SSE.

Those components which are important to reactor operation but not essential to the safe shutdown and isolation of the reactor and whose failure could not result in a release of substantial amounts of radioactivity, but are in close proximity to Category I components, have been seismically qualified to retain limited structural integrity during a SSE, if they have to mitigate the affects of a design basis accident such as a LOCA or steam/feedwater line break.

Category II classification for structures, systems and components is not applicable since the TTC Unit 1 Nuclear Plant was not designed for an Operating Basis Earthquake(OBE) as defined in the Guide for Safety Analysis Report Preparation, Revision 1, October 1972. There are no structures which are partially Category I and partially in a lesser category. Where portions of mechanical systems are Category I and then remaining portions are not seismically classified, the systems have been seismically qualified through the first seismic restraint beyond the defined boundary such as a valve.

All Category I safety-related structures, portions of mechanical systems, and electrical systems and components are listed in Tables 3.2.1-1, 3.2.1-2, and 3.2.1-3, respectively. Category I mechanical fluid components are indicated by the applicable "Seismic Qualification Methods in the column so designated (Table 3.2.1-2). These structures, systems, and components are classified in accordance with Regulatory Guide 1.29 and are designed to remain functional as required to safely shutdown and maintain the reactor in a safe condition after a SSE event.

INSTRUMENTATION

SEISMIC INSTRUMENTATION

LIMITING CONDITION FOR OPERATION

3.3.3.3 The seismic monitoring instrumentation shown in Table 3.3-7 shall be OPERABLE.

APPLICABILITY: At all times.

ACTION:

a. With one or more of the above required seismic monitoring instruments inoperable for more than 30 days, prepare and submit a Special Report to the Commission pursuant to Specification 6.9.2 within the next 10 days outlining the cause of the malfunction and the plans for restoring the instrument(s) to OPERABLE status.

b. The provisions of Specifications 3.0.3 and 3.0.4 are not applicable.

SURVEILLANCE REQUIREMENTS

4 3.3.3. Each of the above required seismic monitoring instruments shall be demonstrated OPERABLE by the performance of the CHANNEL CHECK, CHANNEL CALIBRATION and ANALOG CHANNEL OPERATIONAL TEST at the frequencies shown in Table 4.3-4.

4.3.3.3.2 Each of the above required seismic monitoring instruments actuated during a seismic event greater than or equal to 0.01g shall be restored to OPERABLE status within 24 hours and a CHANNEL CALIBRATION performed within 10 days following the seismic event. Data shall be retrieved from actuated instruments and analyzed to determine the magnitude of the vibratory ground motion A Special Report shall be prepared and submitted to the Commission pursuant to Specification 6.9.2 within 14 days describing the magnitude, frequency spectrum and resultant effect upon facility features important to safety.

3/4.3.3.3 SEISMIC INSTRUMENTATION

The Operability of the seismic instrumentation ensures that sufficient capability is available to promptly determine the magnitude of a seismic event and evaluate the response of those features important to safety This capability is required to permit comparison of the measured response to that used in the design basis for the facility to determine if plant shutdown is required pursuant to Appendix A of 10 CFR Part 100. The instrumentation is consistent with the recommendations of Regulatory Guide 1.12, "Instrumentation for Earthquakes," April 1974.

3/4.3.3.4 METEOROLOGICAL INSTRUMENTATION

The OPERABILITY of the meteorological instrumentation ensures that sufficient meteorological data are available for estimating potential radiation doses to the public as a result of routine or accidental release of radioactive materials to the atmosphere. This capability is required to evaluate the need for initiating protective measures to protect the health and safety of the public and is consistent with the recommendations of Regulatory Guide 1.23, "Onsite Meteorological Programs," February 1972.

3/4.3.3.5 REMOTE SHUTDOWN INSTRUMENTATION

The OPERABILITY of the Remote Shutdown System ensures that sufficient capability is available to permit shutdown and maintenance of HOT SHUTDOWN of the facility from locations outside of the control room and that a fire will not preclude achieving safe shutdown. The Remote Shutdown System transfer switches, power circuits, and control circuits are independent of areas where a fire could damage systems normally used to shutdown the reactor. This capability is required in the event control room habitability is lost and is consistent with General Design Criteria 3 and 19 and Appendix R of 10 CFR Part 50.

3/4 3.3.6 ACCIDENT MONITORING INSTRUMENTATION

The OPERABILITY of the accident monitoring instrumentation ensures that sufficient information is available on selected plant parameters to monitor and assess these variables following an accident. This capability is consistent with the recommendations of Regulatory Guide 1.97, Revision 2, "Instrumentation For light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and following an Accident," December 1980, and NUREG-0737, "Clarification of TMI Action Plan Requirements," November 1980.

Westinghouse Technology Systems Manual

Section 1.2

<u>Introduction to Pressurized Water Reactor Generating Systems</u>

TABLE OF CONTENTS

LIST OF FIGURES

1.2 INTRODUCTION TO PRESSURIZED WATER REACTOR GENERATING SYSTEMS

Learning Objectives:

1. Define the following terms:

    a. Primary cycle,
    b. Secondary cycle, and
    c. Reactor coolant system (RCS) average temperature (T_{avg}).

2. Explain why T_{avg} is programmed to increase with an increasing plant load.

1.2.1 General Description

The pressurized water reactor (PWR) generating system described in this manual is a dual cycle unit. The two cycles are called the primary and the secondary. As shown in Figure 1.2-1, the unit consists of a primary cycle that includes the reactor vessel, the pressurizer and four closed reactor coolant loops connected in parallel (of which only one loop is shown). The secondary cycle includes the steam system, the high and low pressure turbines and the condensate and feedwater system. The secondary systems together are sometimes referred to as the power conversion system. The sole function of the power conversion system is to generate electricity.

As shown, the primary cycle is located entirely inside the containment building. This building is designed to act as a shield to minimize the exposure of radiation to plant personnel. In addition, the design of the containment structure prevents or minimizes the release of radioactive material to the environment during normal operation or under an accident condition. The use of a dual cycle design reduces the amount of radioactive material transferred to the power conversion system components. By minimizing the amount of radioactivity transferred to the secondary, the potential exposure to plant personnel is reduced and any subsequent release of radioactive material to the atmosphere is minimized.

1.2.2 Primary Cycle (Reactor Coolant System)

Each of the four reactor coolant loops contains a reactor coolant pump, a steam generator, piping and associated instrumentation. Attached to one of the four loops is an electrically heated pressurizer. The pressurizer maintains the pressure of the reactor coolant at a high value which prevents the high temperature (>500°F) coolant from boiling. Reactor coolant (pure water with boric acid in solution) is pumped through the reactor core to remove the heat generated by nuclear fission. The heated water exits the reactor vessel, passes through loop piping and enters the steam generator.

Inside the steam generator, reactor coolant flows through U-tubes and gives up some of its heat to the feedwater inside the steam generator (secondary system). The U-tubes act as a barrier between the primary and secondary cycles. Reactor coolant, now cooler, exits the steam generator and is directed to the suction of the reactor coolant pump. The reactor coolant pump returns the reactor coolant to the reactor vessel completing the primary cycle.

1.2.3 Secondary Cycle (Power Conversion System)

The power conversion system begins in the shell side of the four steam generators. At this location the feedwater contacts the U-tubes and picks up heat from the hot reactor coolant. Since the pressure in the secondary side is less than that of the primary, the heated feedwater boils and produces saturated steam. Saturated steam is steam that is at the same temperature of the boiling water for a given pressure.

The saturated steam produced in the shell side of the steam generators exits via the main steam line. The steam flows through a main steam line isolation valve (MSIV) to the high pressure turbine. After flowing through the high pressure turbine, the low-energy, moisture-laden steam is routed to the moisture separator reheaters (MSR's). The MSR, as its name states, removes moisture from this low pressure steam, and reheats it. The moisture-free steam is superheated by heating steam supplied by the main steam system. Superheated steam is steam that is at a temperature which is greater than the saturation temperature at a given pressure. The dry, superheated steam is directed to the low pressure turbines. This steam passes through the low pressure turbine blades and exits to the main condenser. The high and low pressure turbines are mounted on a common shaft that drives the main generator.

The main generator produces electrical power which is supplied to the utility's distribution network or "grid".

Inside the condenser, the exhausted steam is condensed (cooled and depressurized) by passing over tubes containing water from the condenser circulating water system. The condensed steam (now called condensate) is collected in the condenser's hotwell. The condensate is pumped from the condenser hotwell by condensate pumps. The condensate pumps discharge through condensate demineralizers removing impurities from this fluid. The condensate then passes through several stages of low pressure feedwater heating. The temperature of the condensate is increased utilizing the energy of steam extracted from the low pressure turbine. The condensate exits the low pressure feedwater heaters and enters the suction of the high pressure main feedwater pumps.

The main feedwater pumps (normally driven by steam turbines) increase the pressure of this fluid (now called feedwater) so that it can enter the steam generators. From the discharge of the main feedwater pumps back to the steam generators additional feedwater heating is provided by the high pressure feedwater heaters. After this final heating the feedwater passes through the feedwater regulating valves (FRV), enters the containment, and finally into the steam generator, thereby completing the secondary cycle.

1.2.4 Support and Emergency Systems

Attached to each reactor coolant loop cold leg is an accumulator, pressurized with nitrogen. The purpose of the accumulator is to inject borated water into the RCS if the reactor coolant system pressure boundary ruptures, i.e., a Loss of Coolant Accident (LOCA).

When the pressure in the RCS drops below the pressure within the accumulators, the nitrogen forces the borated water out of the accumulator into the RCS providing both water to cover and cool the reactor core and boron (a neutron absorber) to keep the reactor shutdown.

The Residual Heat Removal (RHR) System is designed to provide both safety and non-safety functions. Its safety function is to provide a low pressure, high volume of water into the RCS following a loss of coolant accident. Its non-safety function is to remove decay heat from the core after a shutdown. Decay heat removal is accomplished by pumping hot water from the RCS hot leg through a heat exchanger and then back into the RCS via the cold legs. During a loss of coolant accident, the function of the RHR is to provide cool, borated water from the Refueling Water Storage Tank (RWST) to the RCS for the short term and recycle fluid from the containment building sump back into the reactor coolant system for long term cooling.

The Safety Injection (SI) System is another emergency core cooling system located in the auxiliary building. It's function is to inject borated water from the RWST into the RCS after a LOCA. Although the SI system discharge capacity is much less than that of the RHR, it's discharge pressure is greater.

The Chemical and Volume Control System (CVCS) maintains the purity of the reactor coolant by means of demineralizer beds that continuously purify a small letdown stream from the RCS. This purified water is charged back into the RCS at a controlled rate to maintain the proper volume of water in the RCS. The CVCS charging pumps also serve as the high pressure safety injection pumps. Their function is to supply borated water to the RCS in emergency situations.

In the event of a LOCA, the hot reactor coolant spills from the RCS into the containment and flashes to steam. This action causes a pressure increase inside the Containment Building.

The containment spray system is designed to transfer water from the refueling water storage tank to spray rings located high inside containment. The cool water spraying into the containment, quenches the steam and maintains the pressure inside of the containment to within design limits. This prevents rupture of the containment building and the subsequent uncontrolled release of radioactive materials to the environment.

The Component Cooling Water System (CCW) provides a cooling medium to various components such as the CVCS letdown heat exchanger and the RHR heat exchanger. This system (CCW) is a closed loop system and is cooled by the Service Water System (SWS) which receives its water from a river, lake or ocean. Both of these systems (CCW and SWS) are safety systems and are required to function in order to mitigate the consequences of analyzed accidents.

1.2.5 Plant Layout

The entire RCS, including the steam generators, is located within the containment building. This structure isolates the radioactive reactor coolant from the environment in the event of a leak or a loss of coolant accident. The containment building is designed to withstand the pressure produced by a complete rupture of the largest pipe of the reactor coolant system. In addition, the containment must be able to perform this safety function during and following a "design basis earthquake".* The containment building is therefore designated as a Seismic Category I structure.

* A "design basis earthquake" is also called a "safe shutdown earthquake" and is defined in 10CFR part100 Appendix A of the Code of Federal Regulations. Paraphrasing this part of the code - a design basis earthquake is the maximum ground motion potential considering local and regional geology and seismology. It is that earthquake which produces the maximum vibratory ground motion for which certain structures, systems, and components are designed to remain functional. "Safety related" systems, structures and components designed to remain functional during a design basis earthquake are designated "Seismic Category I".

Safety-related and potentially radioactive auxiliary systems are located inside the Seismic Category I auxiliary building. This building is normally located between the turbine building and the containment building. Ventilation from the auxiliary building is passed through high efficiency particulate filters and/or charcoal filters to minimize the release of radioactive material to the environment. A fuel storage building (sometimes a part of the auxiliary building) is provided for handling and storage of new and spent reactor fuel. The fuel storage building is also designated as a Seismic Category I building. The control building (also sometimes part of the auxiliary building) is a Seismic Category I structure, housing the main control room, the cable spreading room, auxiliary instrument room, plant computer and battery rooms.

The turbine building is not "safety related" and contains most of the secondary cycle equipment and secondary support systems. The main turbine, moisture-separator/reheaters, main condenser, condensate and feedwater pumps, and feedwater heaters, are all located inside the turbine building.

1.2.6 Plant Control

The power output of the reactor and the outlet temperature of the coolant from the reactor core is controlled by manipulating several factors which affect the core's reactivity (neutron production capability). The position of neutron absorbing control rods, the concentration of boric acid in the RCS and the steam flow rate can be changed to affect reactor power and its outlet temperature..

The automatic control systems are designed to provide power change (load change) capability between 15% and 100% of rated power at 5% per minute (ramp) or a 10% instantaneous (step) change in power without causing an automatic reactor shutdown (trip). Additionally, the plant's steam dump system is designed to direct steam to the main condenser allowing the unit to accept a large power reduction (load rejection) without tripping the reactor.

The power level of the reactor is normally changed by selecting a desired electrical load and load rate via the turbine control system and allowing the reactor to follow the turbine load change. Various methods are possible for controlling the reactor's power, as the turbine load is changed, and are discussed below.

1.2.7 Reactor Control

The basic formula defining heat (or power) transferred across a heat exchanger (in this case, the steam generators) is:

$$Q = UA\Delta T$$

where:

Q = heat transferred in BTU's

U = heat transfer coefficient

A = area of heat transfer

ΔT = differential temperature across the heat exchanger or as in this case the difference between the average temperature of the reactor coolant (T_{avg}) and the temperature of the steam (T_{stm}).

For all practical purposes, both the heat transfer coefficient (U), and the heat transfer area (A), are assumed to be constant. Since the heat transfer coefficient is a function of the materials used in the construction of the steam generator and the U-tubes are covered with water. The equation may be reduced to:

$$Q \propto \Delta T$$

or

$$Q \propto T_{avg} - T_{stm}$$

There are three basic modes of reactor coolant temperature control which may be used in a pressurized water reactor. All of these modes of control could be used to adjust reactor power in response to changes in two measurable parameters. These parameters are as follows:

1. T_{avg} is the average reactor coolant system temperature where:

$$Tavg = \frac{T_h + T_c}{2}$$

T_h = Hot Leg temperature,
T_c = Cold Leg temperature, and

2. Steam pressure - The secondary steam pressure either at the outlet of the steam generator or the inlet to the main turbine.

1.2.7.1 Constant T_{avg} Control Mode

With a constant T_{avg} control scheme (Figure 1.2-3), the reactivity of the core is adjusted to maintain a constant reactor coolant average temperature regardless of turbine load. As an example, increasing the output of the turbine causes a decrease in T_{avg} because the turbine uses more energy than that produced by the reactor. The rod control system senses this temperature decrease and withdraws the control rods, adding positive reactivity to the core, returning T_{avg} to program. An anticipatory signal comparing turbine and reactor power might also be utilized to optimize the transient response of this control scheme.

The constant T_{avg} control mode has the advantage of an unchanging RCS temperature and density, regardless of power level. Since the density does not change, pressurizer level is constant for all load conditions.

A major disadvantage of the constant T_{avg} control is that it produces an unacceptable secondary system pressure when the turbine is fully loaded. The amount of heat transferred from the reactor coolant across the steam generator tubes to produce steam depends upon, the heat transfer area of the U-tubes (which is constant), and the differential temperature between the water in the steam generator and the reactor coolant (which is variable). If the reactor coolant T_{avg} and the heat transfer area remain constant then the saturation temperature (T_{stm}) in the shell side (secondary) of the steam generator must drop when the steam demand (load) increases. This effect produces a significant decrease in steam pressure (P_{stm}) as secondary power is increased from hot-zero-power to full load. The low steam pressure produces unacceptable steam conditions at the main turbine inlet.

Large PWR generating stations with U-tube steam generators do not use constant T_{avg} control. The advantage of a constant pressurizer level is greatly offset by the disadvantage of low steam pressure.

1.2.7.2 Constant Steam Pressure Control Mode

With a constant steam pressure control system (Figure 1.2-4), the reactivity of the reactor core is adjusted to maintain a constant pressure in the steam system as turbine load is changed. As described in the previous section, increasing turbine load causes steam pressure (P_{stm}) to decrease. The rod control system would sense this decrease in P_{stm} and withdraw control rods to increase the outlet temperature of the reactor.

With this type of control system, the ΔT between primary and secondary is increased by raising T_{avg} and allowing T_{stm} (and therefore P_{stm}) to remain constant. This produces ideal steam conditions at the main turbine inlet for all loads from hot-zero-power to 100% load.

The disadvantage of this type of control scheme is that it results in a high reactor outlet (hot leg) temperature (T_h), which approaches saturation values. The constant steam pressure control may used in other PWR vendor designs but is impractical for U-tube steam generators.

1.2.7.3 Sliding T_{avg} Control Mode

A sliding T_{avg} control system (Figure 1.2-5) is a compromise between a constant T_{avg} and a constant steam pressure control scheme. This control scheme incorporates the advantages of both but also retains some of their disadvantages.

With a sliding (programmed) T_{avg} control scheme, the reactivity in the reactor core is adjusted to maintain a programmed T_{avg} as the load on the turbine is varied. As with the previously described control systems, varying the load on the turbine causes T_{avg} and steam pressure to increase or decrease. To compensate, the rod control system repositions the control rods to add positive or negative reactivity to the reactor core and maintain T_{avg} equal to its program value.

The energy transferred from the primary cycle to the secondary cycle is directly proportional to the value of the temperature difference (ΔT), between the primary and the secondary. This ΔT is also a direct indication of power. As shown in Figure 1.2-5 as secondary power increases the difference in T_{avg} and T_{stm} increases. The difference between these two (T_{avg} and T_{stm}) is increased by the phenomenon of increasing the load on the turbine generator which causes a steam pressure decrease (thus T_{stm} decreases), and the rod control system responds increasing T_{avg}.

This mode of control produces acceptable steam conditions at the main turbine inlet at 100% power, while requiring a lower Th than that of a constant steam pressure control mode. Most Westinghouse designed nuclear units' use some form of a sliding T_{avg} control program. The difference in the various control programs is the value of the programmed range of temperature control. The programmed average temperature increase varies from a low of 12°F to the most often used value of 30° F. Another difference is in the value of the no-load setpoint (i.e., T_{avg} at 0% power). The most commonly used values of no-load T_{avg} are 547°F and 557°F.

1.2.8 Summary

Pressurized water reactor units use a dual cycle concept, where the closed primary cycle is separate from the secondary cycle. The point of heat transfer between the two cycles is the steam generator(s). The RCS is the primary cycle and is located inside the containment building. Whereas, the secondary cycle includes the steam system, the turbine generator (where steam energy is used to generate electric power) and the condensate and feedwater systems. Secondary cycle systems, subsystems, and components are principally located in the turbine building.

Support and emergency systems generally provide multiple functions to both the primary and secondary. Systems, components, structures, and buildings which have safety functions or are required to maintain the integrity of the RCS or reactor core, under accident conditions, must be built to Seismic Category I standards. Safety systems, components and structures, built to Seismic Category I specifications, will provide their intended safety functions during the maximum credible seismic event.

Reactor coolant temperature control modes such as constant T_{avg} and constant steam pressure are viable control modes but are not generally used in the Westinghouse design. The control scheme most often selected to control the temperature of the reactor coolant is the sliding T_{avg}. This mode of control programs T_{avg} to increase as secondary load increases. The sliding T_{avg} mode is a compromise between the other two modes of control and contains some of the advantages and disadvantages of each.

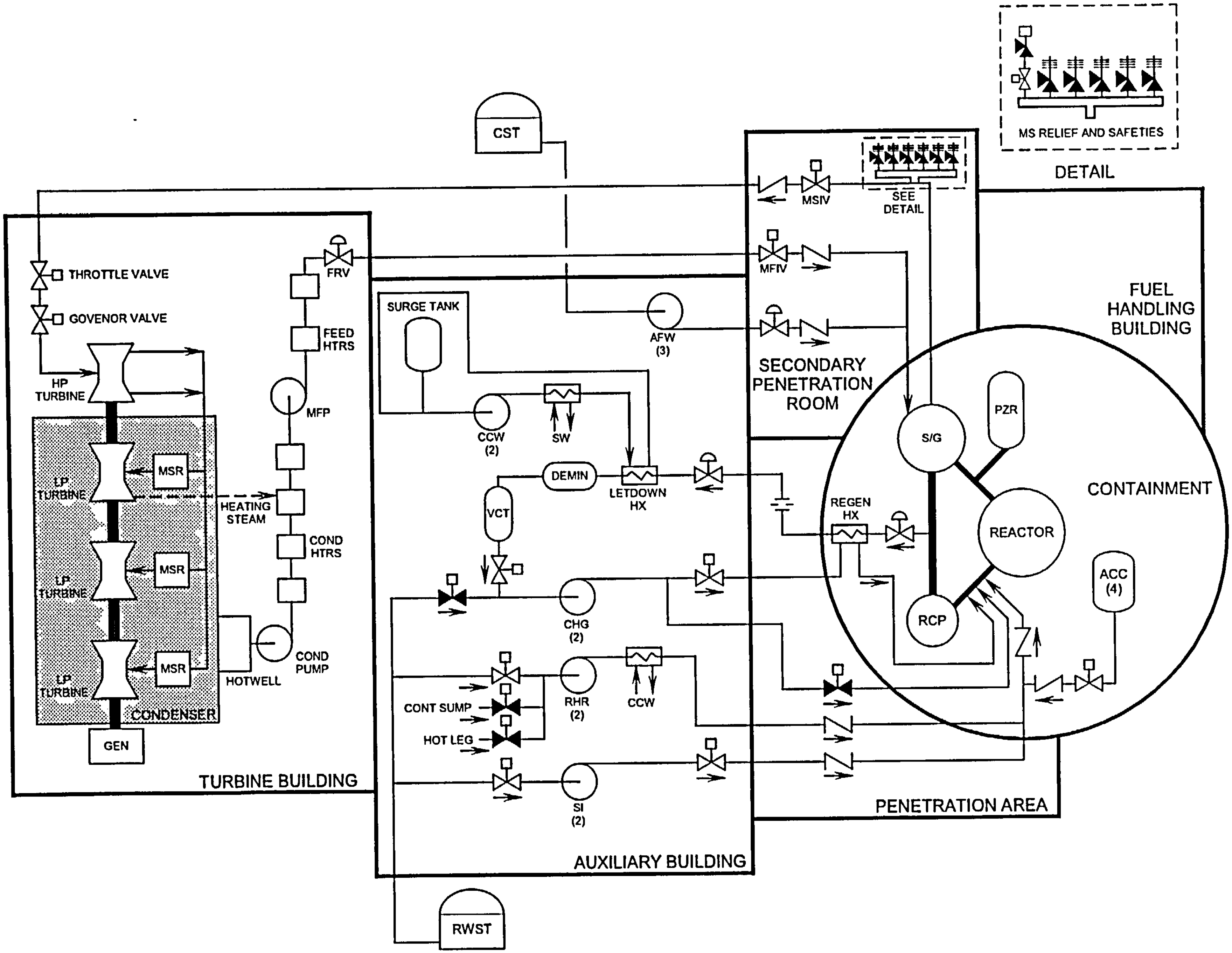


Figure 1.2-1 Plant Systems Composite

1101-329
12-1, 1-2

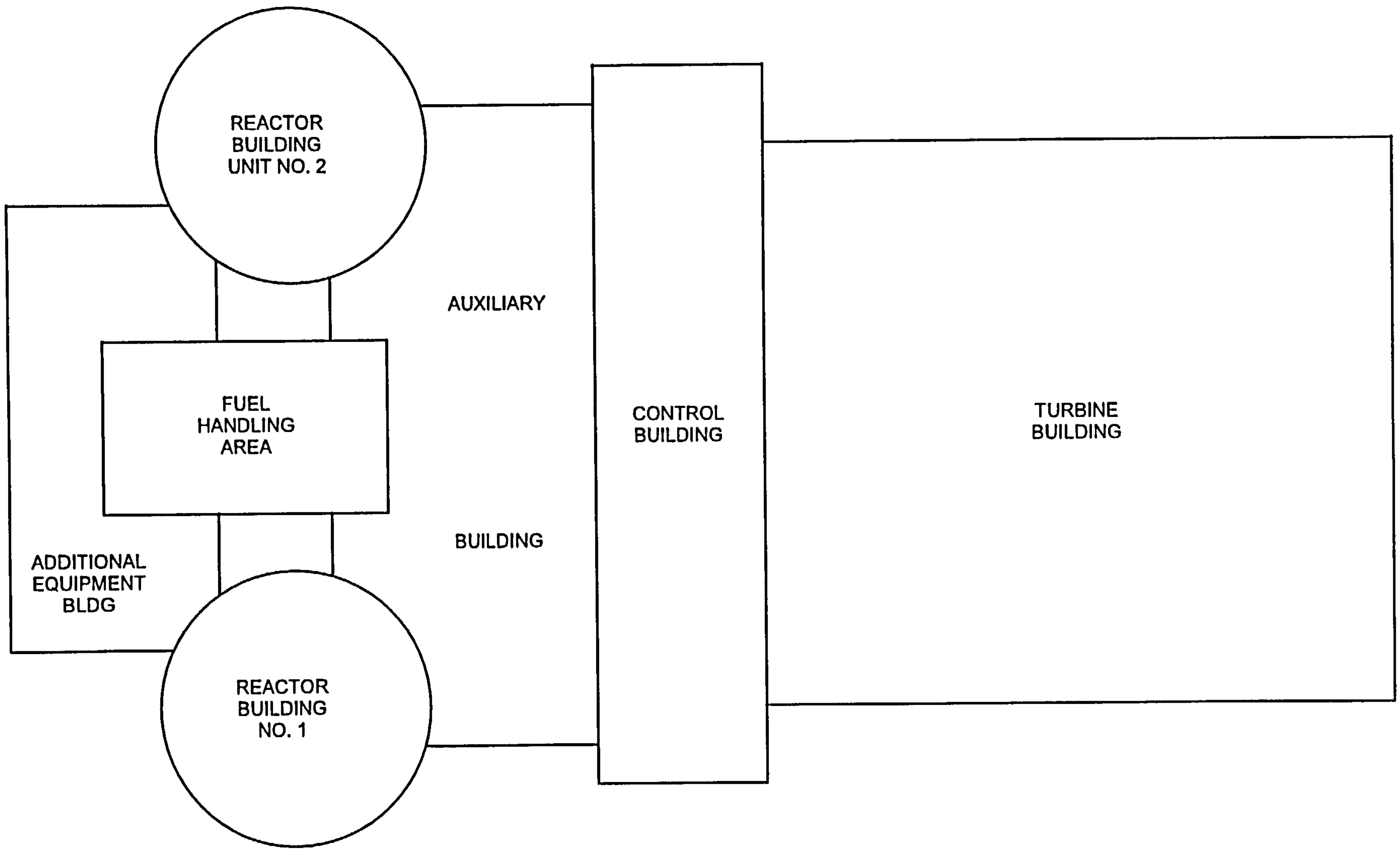
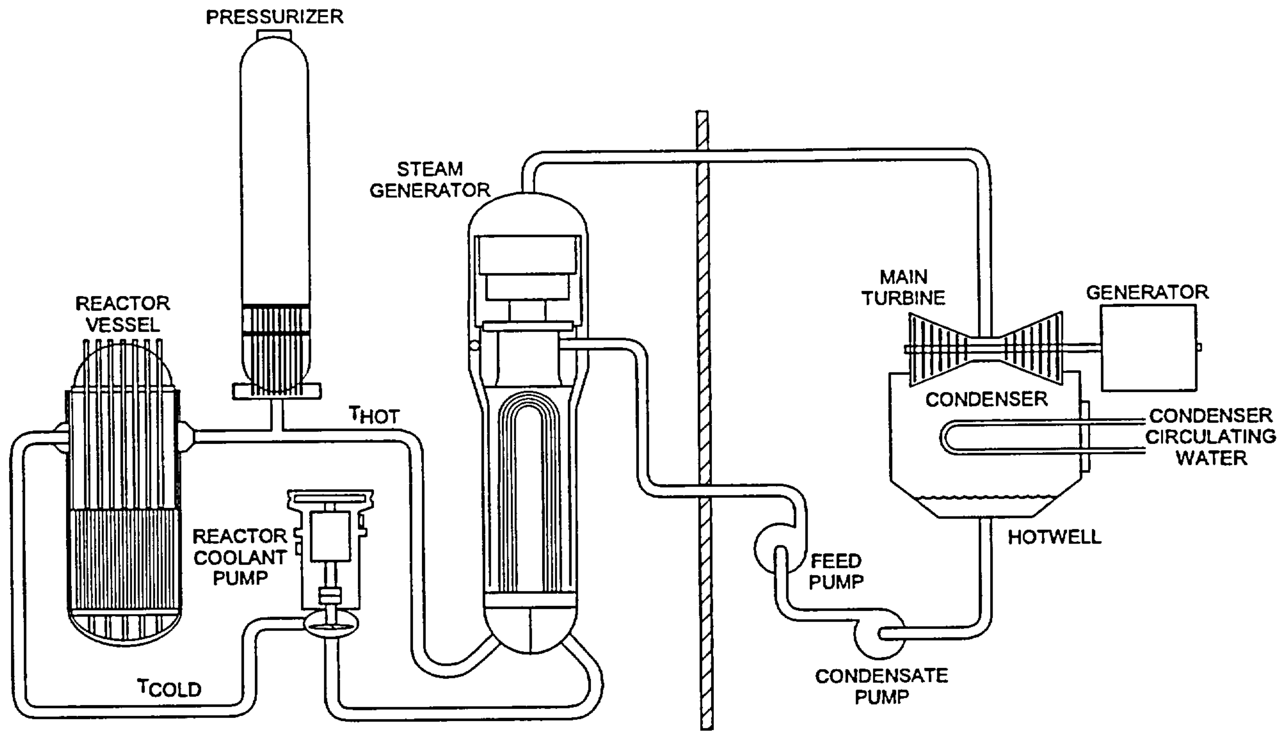


Figure 1.2-2 Plant Layout

0199-3



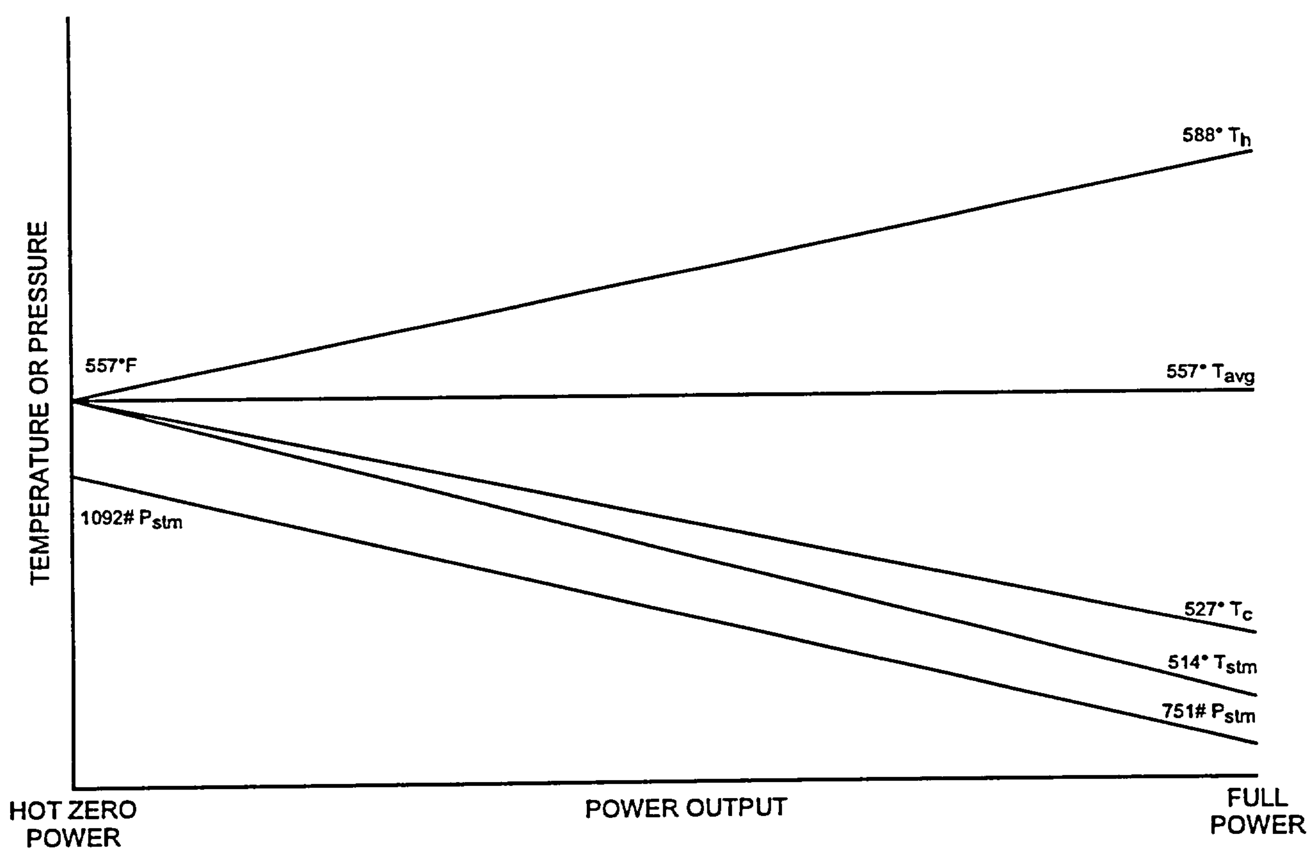


Figure 1.2-3 Characteristics of a Constant Average Temperature Program

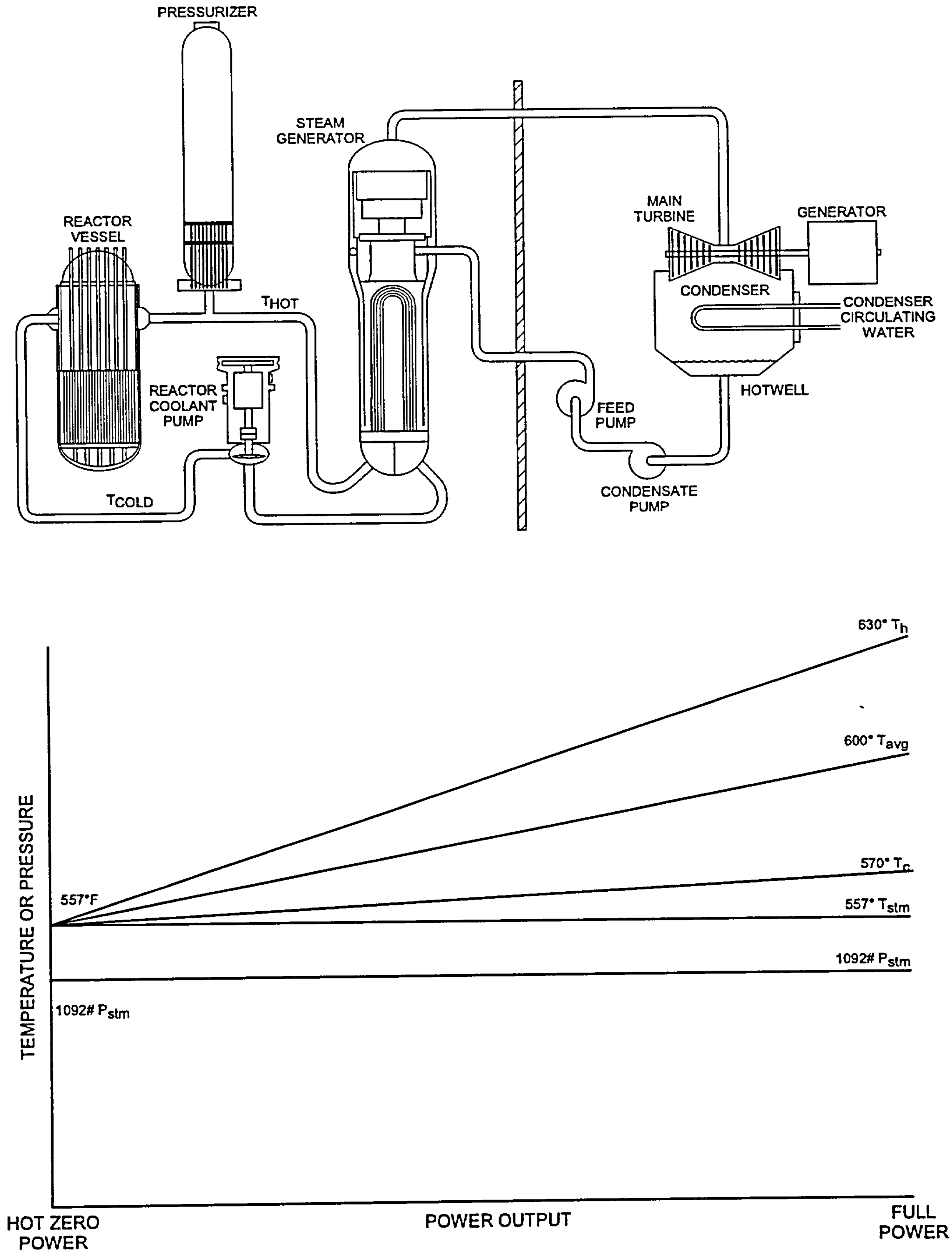
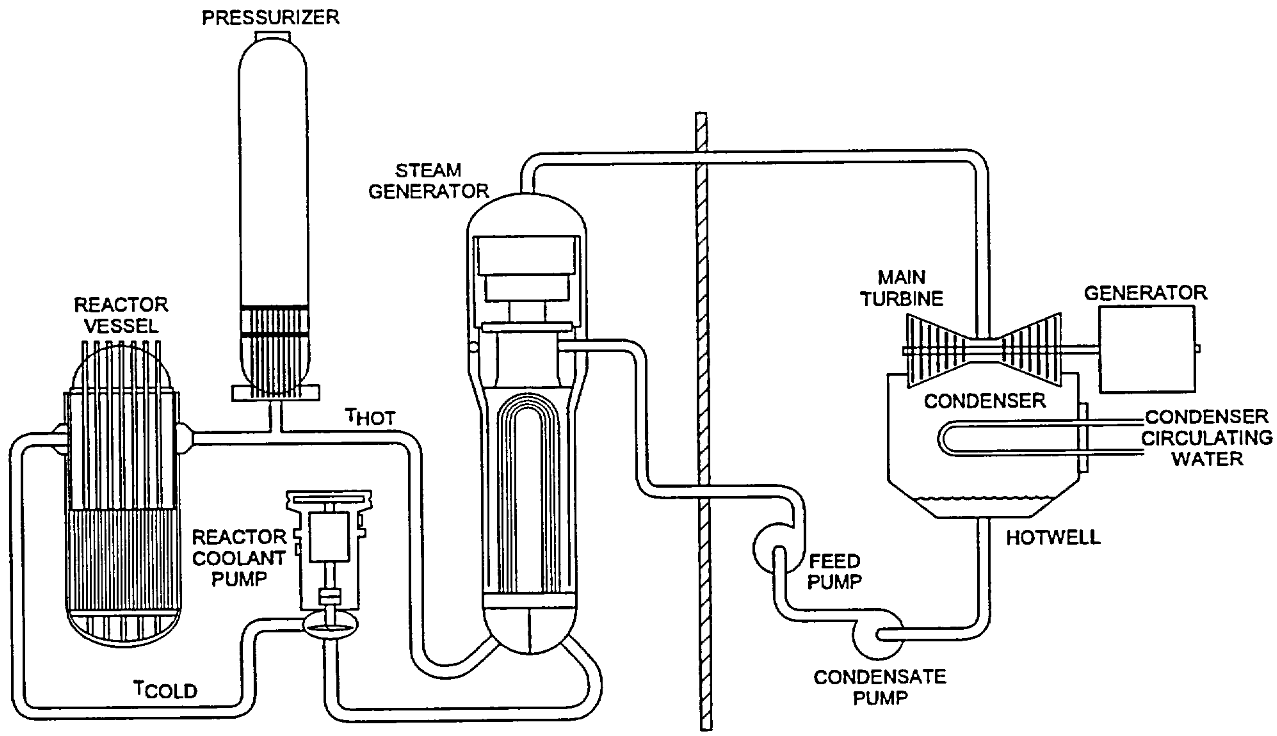


Figure 1.2-4 Characteristics of a Constant Steam Pressure Program



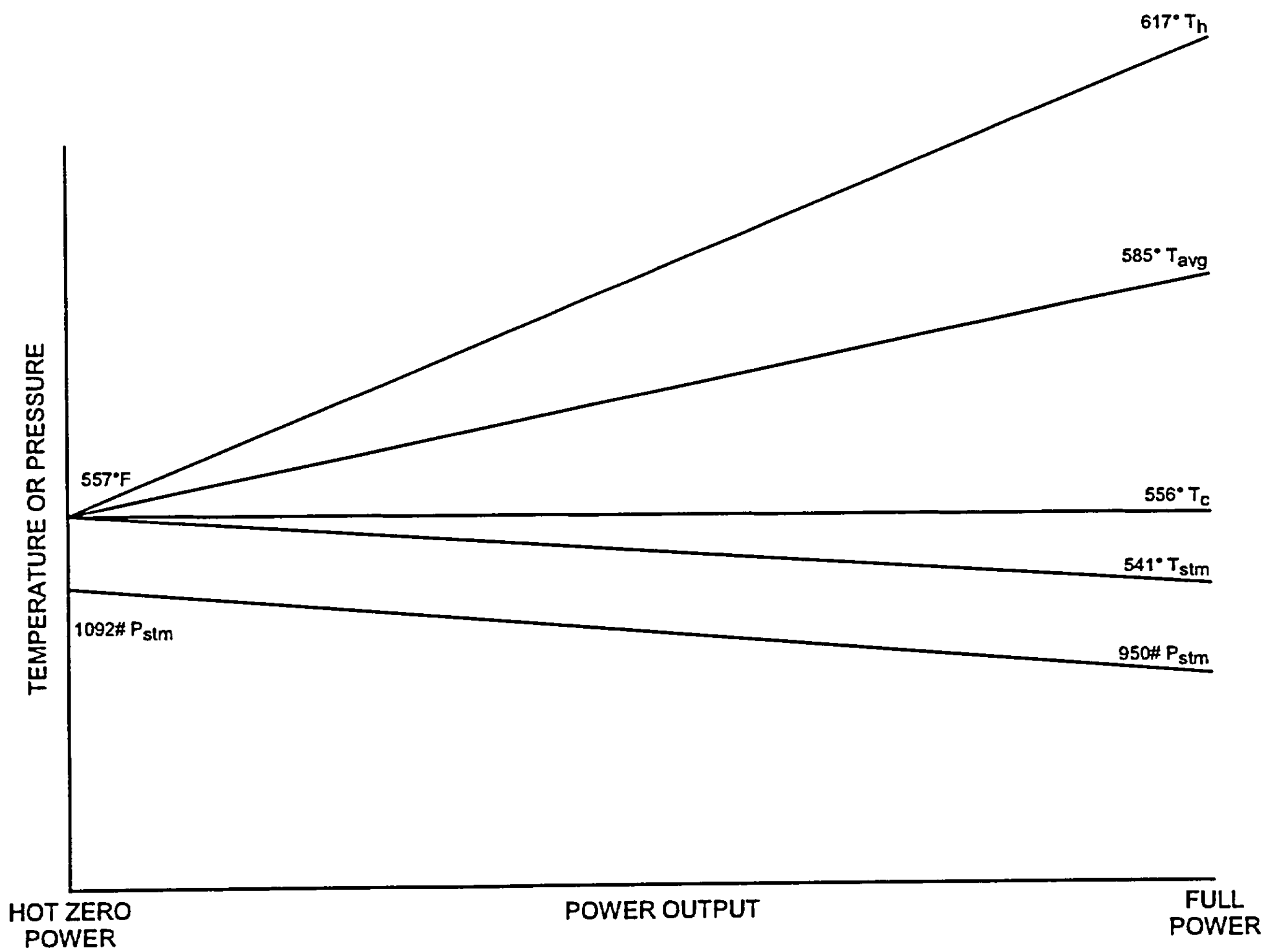


Figure 1.2-5 Characteristics of a Sliding Average Temperature Program

Westinghouse Technology Systems Manual

Section 1.3

Instrumentation and Control

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1.3 INSTRUMENTATION AND CONTROLS

Learning Objectives:

1. Describe the type of sensing instruments used to sense pressure, temperature, and flow.

2. Explain how the properties of pressure, temperature, and flow are converted into electrical outputs.

3. Explain how the following controllers respond to a step change and ramp change in input:

   a. bistable
   b. proportional
   c. proportional plus integral
   d. proportional plus derivative

4. Explain the input and output relationships of the standard logic circuits.

1.3.1 Introduction

This section addresses the detection of process variables and the conversion of these measured values into electrical or pneumatic signals. These signals will then be used for indication and control functions. The basic controllers used in power plant control systems will be discussed including their response to various input signals. In addition, a brief discussion of simple logic circuits will conclude this section.

1.3.2 Pressure Sensing Instruments

Pressure, defined as force per unit area, is one of the measured and controlled properties. Pressure measurements range from the high pressure of the reactor coolant system measured in pounds per square inch (psi) to the vacuum in the main condenser measured in inches of mercury (in. Hg.). The devices listed in this section are used for the measurement of system pressure.

1.3.2.1 Bourdon Tube

The simple bourdon tube, shown in Figure 1.3-1, consists of an oval tube rolled into an arc of a circle. One end is open to the process variable to be measured and the other end is closed. The surface area on the outer portion of the arc is larger than the surface area of the inner portion, and when pressure (force per unit area) is applied, the tube tends to straighten out very slightly. If the pressure is removed, the elasticity of the tube causes its to return to its original shape. The pressure of the fluid is converted to a mechanical motion by the bourdon tube. This motion can be converted into an electrical or pneumatic signal, or can drive a pointer on a local indicating gage for measurement of the applied pressure. The helical element, shown in Figure 1.3-2(b), is a variation of the simple bourdon tube. It is similar to the bourdon tube except that it is wound in the form of a spiral containing four or five turns. The helical element amplifies the movement of the closed end of the bourdon tube. The spiral type of measuring element is a second modification (Figure 1.3-2(a)) of the bourdon element. It is a thin-walled tube that has been flattened on opposite sides to produce an approximately elliptical cross section. The tube is then formed into a spiral. When pressure is applied to the open end, the tube tends to uncoil.

1.3.2.2 Bellows Pressure Sensor

The bellows pressure sensor, shown in Figure 1.3-3(a), is made up of a metallic bellows enclosed in a shell, with the shell connected to a pressure source. Pressure acting on the outside of the bellows compresses the bellows and moves its free end against the opposing force of the spring. A rod attached to the bellows transmits this motion to the pressure transmitter.

1.3.2.3 Diaphragm Pressure Sensor

The diaphragm pressure sensor, shown in Figure 1.3-3(b) consists of a metallic diaphragm (rigidly supported at each end), a spring, and a force bar that is connected to the diaphragm. When pressure is applied, the diaphragm moves in opposition to the spring, which causes motion of the force bar. When pressure is removed, the elasticity of the diaphragm and action of the spring return the sensor to its zero pressure condition.

1.3.2.4 Mechanical to Electrical Signal Conversion

In the sensors described above, the application of pressure results in a mechanical signal. Two devices are available for the conversion of this mechanical signal into an electrical signal that can be used in the plant control or protection systems. The use of one device, the force balance transmitter, results in a current (milliampere, ma) output; the use of the other device, the movable core transformer transmitter, results in a voltage output.

Force Balance Transmitter

Force balance refers to the system whereby the free motion of the sensor is limited and actively opposed by some mechanical or electrical means. In Figure 1.3-4 a simplified force balance transmitter is shown. As pressure increases, the diaphragm is moved to the left. This motion, in turn, causes movement of the force bar (the force bar is pivoted at the sealed flexure). The force bar motion causes movement of the reference arm, which closes the gap between the error detector transformer coils and the ferrite disk attached to the reference arm. When the gap of the error detector becomes smaller, the magnetic coupling between the transformer coils increases, increasing the output of the error detector transformer. The output of the error detector is amplified and applied to the force feedback coil. The increased current in the force feedback coil exerts a greater pull on its armature moving the reference arm in the opposite direction, thus restoring the system balance. The amount of current required to maintain the system in balance is proportional to pressure and, therefore, can be used in the indicating and control loops. Two current ranges, 4 to 20 ma or 10 to 50 ma, are generally used for this transmitter's output circuitry.

Movable Core Transmitter

In the movable core transmitter, show in Figure 1.3-5 the pressure sensor's mechanical linkage is connected to the core of a linear variable differential transformer (LVDT). The LVDT consists of a primary coil and two secondary coils. The movement of the core changes the magnetic flux coupling between the primary coil and the secondary coils which, in turn, causes a change in the voltage output of the secondary coils. The secondary coils are connected in series opposition so that the two voltages in the secondary circuit have opposite phases. With the core in the center position of the transformer, the voltage output is zero. This will give a normal voltage range of -10 to 0 to +10 v.

Variable Capacitance Transmitter

Another type of transmitter is being installed at nuclear power plants currently under construction. This type of transmitter is called a variable capacitance transmitter (see Figure 1.3-6) and consists of a set of parallel capacitor plates with a sensing diaphragm placed between the plates. The capacitor is filled with silicon oil. The need for a pressure-sensing element, such as a bellows or bourdon tube, and its mechanical linkage has been eliminated by connecting the process fluid to a separate isolating diaphragm.

One side of the isolation diaphragm is in contact with the process stream, while the other side is in contact with the silicon fill oil. When pressure is applied to the isolating diaphragm, the force is transmitted through the silicon oil to the sensing diaphragm causing it to deflect. The deflection of the sensing diaphragm is detected by the capacitor plates. The change in capacitance, because of sensing diaphragm deflection, is converted to a 4 to 20-mA output that is transmitted to the plant protection and/or control systems.

1.3.3 Flow Sensing Instruments

Selected pressure detection devices may be used to provide a reliable measurement of process flow. To measure flow in this, manner, a differential pressure (ΔP) is created by some type of primary device, such as an orifice plate, a flow nozzle, or a flow venturi. Flow rate measured in this manner is proportional to the square root of the ΔP. The ΔP is sensed and converted from a mechanical movement to an electrical signal for flow measurement.

1.3.3.1 Primary Devices

Orifice Plate

The orifice plate, Figure 1.3-7(a), in its most common form, is merely a circular hole in a thin, flat plate that is clamped between the flanges at a joint in the system piping. The orifice plate is inexpensive and accurate, but as shown in Figure 1.3-7(a) it has poor pressure recovery.

Flow Nozzle

The flow nozzle, Figure 1.3-7(b) provides better pressure recovery (i.e., less pressure loss) than the orifice plate. It consists of a rounded inlet cone and an outlet nozzle.

Flow Venturi

The flow venturi, Figure 1.3-7(c), has the best pressure recovery characteristics and is used in those systems where a high-pressure drop across the primary element is undesirable. The venturi consists of rounded inlet and outlet cones connected by a constricted middle section. As the velocity increases in the constriction, the pressure decreases. A pressure tap is provided in this low-pressure area.

1.3.3.2 Bellows Flow Sensor

The bellows flow sensor (Figure 1.3-8) consists of two bellows: one that senses the high side (inlet) pressure of the primary device and another that senses the low side (outlet) pressure of the primary device. The difference in force exerted by the two bellows is proportional to the differential pressure developed by the primary element. A mechanical connection is made to the force bar of the force balance transmitter or the core of the movable core transformer (Paragraph 1.3.2.4) to convert the differential pressure signal to an electrical signal. Since the flow rate is proportional to the square root of the ΔP, a square root extractor circuit is required to convert the electrical output into flow indication.

1.3.3.3 Diaphragm Flow Sensor

Again, the principle of opposing forces created by the differential pressure across the primary device is used to sense flow with the diaphragm flow sensor (Figure 1.3-9). The displacement of the diaphragm causes motion of the force bar of the force balance transmitter or the core of the movable core transformer (Paragraph 1.3.2.4) and converts the ΔP signal to an electrical signal. A square root extractor is again required. The majority of the flow transmitters in the plant use diaphragm flow sensors.

1.3.3.4 Magnetic Flow Sensors

Unlike the previous flow sensors discussed in this section, the magnetic flow sensor (Figure 1.3-10) does not require a primary element. The magnetic flow transmitter works on the principle that voltage can be generated if relative motion exists between a conductor and a magnetic field. The liquid is used as the conductor. The flow transmitter generates the magnetic field, and the flow of the liquid provides relative motion. Electrodes located in the piping detect the generated voltage.

1.3.4 Level Sensing Instruments

Most measurements of level are based on a pressure measurement of the liquid's hydrostatic head. This hydrostatic head is the weight of the liquid above a reference or datum line. At any point, its force is exerted equally in all directions and is independent of the volume of liquid involved or the shape of the vessel. The measurement of pressure as a result of level head can be translated to level height above the datum line as follows:

$H = P/\rho$ (1.3-1)

where:

H = height of liquid

P = pressure resulting from hydrostatic head

ρ = density of liquid.

Different pressure sensors, both bellows and diaphragm (Paragraphs 1.3.3.2 and 1.3.3.3) are used to sense level. On tanks that are vented, the low side of the differential pressure sensor is open to atmospheric pressure. Pressurized tanks such as the core flood tanks have reference legs that tap into the gas space of the tank; therefore, the level indication is not affected by changes in tank pressure. The pressurizer and steam generators use a filled (wet) reference leg, and level (ΔP) is sensed in accordance with the following equation:

$\Delta P = H_r\rho_r - H_v\rho_v$ (1.3-2)

where :

H_r = height of the reference leg

ρ_r = density of the reference leg

H_v = height of the variable leg

ρ_v = density of the variable leg

The reference legs are kept full by condensate pots that tap into the steam space of both vessels. It should be noted from the above formula that a density change in either the reference or variable leg will affect the ΔP that is seen by the sensor; also when the vessel is full, the ΔP is equal to zero. Both flow and level sensors are referred to as differential pressure cells or transmitters.

1.3.4.1 Variable Capacitance Differential Pressure Transmitters

A detector similar in construction to the variable capacitance pressure detector (Paragraph 1.3.2.5) is used to measure the differential pressure caused by level or flow. As seen in Figure 1.3-11, two isolating diaphragms (one diaphragm for the high-pressure input and one diaphragm for the low-pressure input) are used. The differential pressure exerts a force through the silicon fill oil to change the position of the sensing diaphragm. The change in sensing diaphragm position is detected by the capacitor plates. The change in capacitance is electronically converted to a 4 to 20 mA output.

1.3.5 Temperature Sensing Instruments

Temperature is one of the most measured and controlled variables in the nuclear plant. Uses of temperature measurements range from inputs into the reactor protection system to measurement and control of the chilled water temperature from the station air conditioning system. Three basic types of temperature detectors are used, the fluid-filled system, the thermocouple, and the resistance temperature detector. Each of these temperature detectors is discussed in the following sections.

1.3.5.1 Fluid-Filled Systems

Fluid-filled temperature sensors are usually gas-filled "pressure" detectors (Figure 1.3-12). When the temperature of a gas changes, its pressure also changes. The pressure change of the gas is sensed by a bourdon-tube-type pressure sensor, in which the bourdon tube is connected to a pointer that travels across a scale calibrated in temperature units. The primary use of these systems is local temperature indication.

1.3.5.2 Thermocouples

When two dissimilar metals are welded together and this junction is heated, a voltage is developed at the free ends. The magnitude of the voltage is proportional to the temperature difference between the hot and cold junctions (see Figure 1.3-13) and a function of the types of materials used in thermocouple construction. Because connections must be made to the thermocouple at the cold junction and at the measuring device, all thermoelectric systems consist of three separate thermocouples: the thermocouple proper, the external lead wire, and the reference junction. The voltage developed in the circuit is then a combination of the voltages generated by all three junctions. If the temperature at the reference junction changes, the total voltage of the circuit changes, and the proportionality between the process temperature and measured voltage is destroyed. The temperature of the reference junction must be kept constant, or changes in this temperature may be compensated for by a temperature sensitive resistor. The temperature sensitive resistor will provide a voltage drop in the circuit to compensate for reference junction temperature changes. The incore system uses thermocouples as temperature sensors.

1.3.5.3 Resistance Temperature Detectors

In Figure 1.3-14, a typical bridge circuit is shown. The bridge consists of three known resistances and the resistance temperature detector (RTD). The RTD's resistance varies with temperature: as temperature increases, the resistance of the RTD also increases. As the resistance of the RTD changes, the voltage difference between points A and B of the bridge circuit changes. This voltage difference is proportional to the temperature that is sensed by the RTD and is used as an input to the indication and control circuits. The RCS hot- and cold-leg temperature detectors are RTDs.

1.3.6 Controllers

In order to control some physical process, (Figure 1.3-18) at least three items must be considered. First, the desired value of the parameter must be chosen. This desired value is called the setpoint for the control system and may be supplied either manually or as a function of a related variable. Second, the actual value of the process must be known. The input of this variable is provided by a detector which senses the value of the process that is to be controlled. Finally, some device must be installed to cause the parameter to achieve its desired value. This device will be controlled by the difference between the setpoint and actual value of the process. The difference between the setpoint and actual value of the parameter is derived in a summing circuit (Σ) and is called an error signal.

The simplest form of a controller is called a Bistable. A bistable turns on or off in response to a control signal. For example a bistable can be used in the control system of a process instrument. In the pressurizer heater control system a bistable controls the operation of the pressurizer heaters in response to pressurizer level. At 17% or less pressurizer level the pressurizer heaters are deenergized. This is in response to the pressurizer level instrument . At 17% level a bistable turns off preventing operation of the pressurizer heaters in a steam environment. Once pressurizer level is greater than 17% the operator can restore the operation of the pressurizer heaters.

1.3.6.1 Proportional Control

In this Paragraph, the basic concepts of a control system will be applied to a hypothetical process. It is desired to control the level in a tank (Figure 1.3-19) at a constant value. This tank has an inlet supply of water and a valve installed on the outlet line. A level setpoint of 50% has been chosen and a level transmitter (detector) with the capability of measuring the contents of the tank over the range of 0 to 100% has been installed. The controlled device is the outlet control valve. The following assumptions are made:

1. The inlet flow to the tank can be varied to introduce a disturbance into the system.
2. The outlet flow through the control valve can match inlet flow.
3. The output of the controller will be a value equal to 50% when the tank level is at setpoint, i.e., the error signal is equal to zero.
4. There exists a one to one correspondence between controller output and valve position.

Initial conditions are the tank level at 50% with a given inlet flow equal to outlet flow. Since the tank is at 50% level, the controller output and outlet control valve position are also at 50%, Figure 1.3-19(b). The change in controller output for a change in tank level is represented by the 45° line. Now consider the response of the system if inlet flow is suddenly stopped. First of all, with no inlet flow and the outlet valve positioned at 50%, tank level will drop. As tank level starts to drop, the output of the level transmitter starts to change. In the summing unit (Σ) the change in transmitter output will be sensed resulting in an error signal, Figure 1.3-19(c). The error signal causes a change in controller output which, in turn, causes the outlet valve to start to close. The decrease in tank level will not be terminated until the outlet valve is fully closed and this will occur when the controller output is zero. Unfortunately the output of the controller will equal zero only when the tank is empty. An empty tank falls far short of the goal of controlling tank level at 50%. Conversely, if the level in the tank was at 50% and the inlet flow was increased to its maximum value, then inlet flow would be greater than outlet flow causing tank level to increase.

The increase in tank level is sensed by the level transmitter. The change in the output of the level transmitter is compared with the setpoint in the summing unit (Σ) resulting in an error signal. The error signal causes an increase in the output of the controller resulting in the opening of the outlet control valve. In order to stop the increase in tank level, the outlet valve must be fully open. The outlet valve will be 100% open when the tank is full. Again, the control system will not control the tank level at setpoint. From these two examples, it is evident that the controller will not operate correctly in its present configuration. However, if the output of the controller can be increased by a value that is proportional to the change in the error signal, then the outlet valve will achieve its required position sooner. This will prevent gross oscillations in tank level. Such a controller is called a proportional controller because its output is proportional to the input error signal.

output = (k) (error signal)

where:

k is the proportionality constant.

To illustrate the affect of the proportionality constant, values of k equal to 2 and .5 will be arbitrarily chosen while maintaining a 50%

controller output with a zero error signal. As shown in Figure 1.3-19(a) with k equal to 2, if the error signal increases by 25% then the output of the controller will increase to 100%. In the opposite direction a change in the error signal of 25% will result in a controller output of 0%. Formally k is called the "gain" of the controller and is defined as follows:

Gain = Δ output / Δ input

The output of the control system versus tank level for the two different values of gain is shown in Figure 1.3-19(b). The effects of these two values of gain will be examined with perturbations in inlet flow.

Note on Figure 1.3-19(c) that tank level is at 50% (setpoint). At time t=1, the inlet flow is stopped. With output flow greater than inlet flow, tank level begins to decrease. The decrease in tank level will continue until the outlet valve is fully closed. The value of tank level resulting in closure of the outlet valve can be determined from Figure 1.3-19(b). With a gain of 2 the valve will be closed when tank level is 25%. At time t=4, inlet flow is increased from zero to its maximum value. Since inlet flow is greater than outlet flow, tank level will rise.The increase in tank level will stop when outlet and inlet flows are equal. This will occur when the outlet valve is 100% open. Again, the tank level corresponding to the full open valve position can be determined from Figure 1.3-19(b). Since the controller has a gain of 2, the level increase will be stopped at 75%.

Table 1.3-1
Gain and Proportional Band

Gain	Proportional Band (in %)
0.5	200%
1.0	100%
2.0	50%
5.0	20%

Now, using a gain of 5 for the same conditions as described above with the previous gain of 2. At time t=1, with the tank level at 50% (setpiont), the inlet flow is stopped. With output flow greater than inlet flow, tank level begins to decrease. The decrease in tank level will continue until the outlet valve is fully closed. The value of tank level resulting in closure of the outlet valve can be determined from Figure 1.3-19(c). With a gain of 5 the valve will be closed when tank level is 40%. When k is equal to 5, changes in the error signal of -10% to +10% correspond to controller output of 0% and 100% respectively. With a gain of 5, the increase in tank level will be terminated at 60%.

It should be noted that tank level is not controlled at setpoint in either case. This is a characteristic of a proportional controller. A proportional controller will not control at setpoint because a change in the error signal is required to cause a change in the output of the controller. Although the proportional controller will not control at setpoint, it will control within a band around the setpoint. This leads to the definition of the proportional band (PB). The proportional band of a controller is the change in input required to cause a 100% change in the output. The proportional band is the reciprocal of gain as illustrated on Figure 1.3-19(c) and the following:

At a glance it would appear that increasing the gain would cause the controller to control closer to setpoint. While this is true, limitations on gain do exist. Equipment or process time delays must be taken into consideration when choosing values of gain.

1.3.6.2 Proportional Plus Integral Control

In order to eliminate the proportional controller's offset between the actual value of the parameter and the process setpoint, integral control action is added to the control system (see Figure 1.3-20). The integral action eliminates the offset by integrating the proportional band and adding this signal to the controller output. Prior to examining the operation of integral action, two terms need to be defined. The first term is "reset rate" and is defined as the number of times the magnitude of the change in controller output caused by the proportional band deviation will be added to the controller output per unit time. Reset rate is expressed in repeats per minute (RPM). The other term is "reset time" and is defined as the time required to repeat the magnitude of the change caused by the proportional band action. Reset rate and reset time are reciprocal terms. To illustrate this, assume a controller has a proportional band of 200% (gain = 0.5) and a reset rate of 2 RPM. If a step change of 20% occurs in the process variable, the magnitude of the change in the controller output due to proportional band action is 10%. A reset rate of 2 RPM will cause a change of an additional 20% every minute the error exists. A reset rate of 2 RPM corresponds to a reset time of 0.5 minutes; therefore, the output of the controller will be changed an additional 10% every 30 seconds.

For review the actions of the control system in response to a step change from 50% to 70% with a gain of 0.5 and a reset rate of 1 RPM are as follows:

1. The controller output due to proportional controller action will increase from 50% to 60% (20% Δ input x 0.5 gain = 10%).
2. The change of 10% due to proportional action will cause a change of 10% every minute for a 1 RPM reset rate.
3. The output of the integral action will be combined with the output of the proportional controller to cause a greater opening of the tank outlet control valve for each percent level error.
4. A greater opening of the control valve will increase the outlet flow from the tank. If outlet flow is increased, then tank level will decrease.
5. As the level decreases, the output of the controller will decrease closing down on the outlet control valve. This action will continue until the setpoint of 50% is reached.

Now using the same initial conditions as above with the exception that the reset rate will be 2 RPM in this example. The actions of the control system in response to a step change from 50% to 70% with a gain of 0.5 and a reset rate of 2 RPM are as follows:

1. The controller output due to proportional controller action will increase from 50% to 60% (20% Δ input x 0.5 gain = 10%).
2. The change of 10% due to proportional action will cause a change of 20% every minute for a 2 RPM reset rate.
3. The output of the integral action will be combined with the output of the proportional controller to cause a greater opening of the tank outlet control valve for each percent level error.
4. A greater opening of the control valve will increase the outlet flow from the tank. If outlet flow is increased, then tank level will decrease.
5. As the level decreases, the output of the controller will decrease closing down on the outlet control valve. This action will continue until the setpoint of 50% is reached.

The addition of integral action to the controller will achieve the desired result of having the control system control at setpoint because controller output will continue to change as long as an offset between the actual value of the parameter and its setpoint exists. As the value of the controller changes, the controlled device will be modulated. This action will restore the parameter to setpoint.

1.3.6.3 Proportional Plus Derivative Control

The installation of derivative action into the control scheme gives the system the ability to start action based upon the rate of change of the control systems input. This is sometimes referred to as an anticipatory circuit. A derivative controller "anticipates" the change in the process variable by the addition of a signal that is proportional to the rate of change of the input signal. The change in controller output due to derivative action is called "rate gain" and is defined as the multiplication of the change in proportional action due to a step change in the process parameter. A step change is used here as a reference condition.

As an example, if a step change of 10% causes a proportional controller's output to change by 5% (200% proportional band), then the addition of derivative action with a rate gain of 5 would cause an additional increase in the controllers output of 25%. Figure 1.3-21 illustrates the effects of adding derivative action to the control system. Inlet flow to the tank is adjusted to give a rate of increase in level of 10% per minute It will be assumed that the increase in controller output does not decrease the rate of level increase (no feedback). As tank level begins to increase at a rate of 10% per minute, the output of the controlle due to proportional action begins to increase at 5% per minute (gain times the change in input). The rate of change of level is constant; therefore, the output of the derivative circuit will increase from 0% to 10% (rate gain of 2 times the 5% change in output due to proportional band action) and remain constant.

The increase in controller output positions the level control valve to a greater opening per percent level error restoring tank level to setpoint sooner. A comparison of the proportional control output graph, and the proportional plus derivative graph, shows that the time required to reach a particular controller output is decreased by the addition of derivative action. This reduction in time is called "rate time" and is defined as the decrease in time it would take the controller output to reach the same value that would be obtained by only proportional action when the process parameter is changing from setpoint at a constant rate.

Figure 1.3-21 shows a transient involving a step change in tank level. The step change causes an increased controller output due to proportional plus derivative action. After the step change has occurred, the rate of change of level deviation is zero. This causes the derivative signal to be reduced to zero over a given period of time.

The time required for the output to decay by 63.2% of the signal due to the action of the derivative portion of the controller is called the "time constant." The output of the controller is an exponential function and will change by 63.2% of the controllers maximum value in one time constant. The output of the derivative portion of the controller will equal zero after 5 time constants. If the deviation between setpoint and the process parameter, as shown in Figure 1.3-21 is increasing, the portion of the controller output due to derivative action will reach its steady state value in five time constants.

1.3.6.4 Proportional Plus Integral Plus Derivative (PID) Controllers

The proportional plus integral plus derivative (PID) controller is the most sophisticated controller used in the power plant and can be used to summarize the previous types of controllers. The proportional component of the PID provides an output that is proportional to its input. The input signal to the controller is the error that results from the comparison of the actual value of the parameter and its desired value (setpoint).

The proportionality constant is called gain. Since a change in the input is required to cause a repositioning of the controlled device, an inherent offset would exist. The addition of the integral portion of the PID controller eliminates the offset of the proportional action. The integral portion of the controller accomplishes this function by adding the integral of the proportional deviation to the output of the controller. This increase in controller output changes the status of the controlled device and causes the process parameter to achieve the desired value. Finally, the derivative action adds an anticipatory feature to the controller. This anticipatory feature is performed by adding a signal to the controller output that is proportional to the rate of change (the derivative) of the proportional band deviation. Response of the PID controller to various input signals without feedback is shown on Figure 1.3-21.

1.3.7 Logic Diagrams

The concept of logic diagrams was introduced to provide complete system information to personnel in an easily interpreted format. These diagrams, through the use of standard symbols, explain specific system or component control, protection and operational capabilities without requiring detailed research of complex electrical or mechanical system diagrams. With the use of a few standard symbols and a basic knowledge of the system's functions and capabilities, a large quantity of useful information may be obtained. To illustrate the concept of logic diagrams and their component parts, the basic symbols will be introduced and briefly discussed and an example given of their application.

The symbols to be discussed will not be all inclusive; however, those discussed are the most common. In every case of logic diagram usage by a vendor, architect engineer, or utility, an explanation sheet of symbols is included.

1.3.7.1 "OR" Logic

The "OR" logic is represented in Figure 1.3-26(a). This logic symbolizes an input and an output function. In the "OR" logic flow, any input signal is considered to be passed through to produce an output. The loss of all inputs will cause a loss of the output.

1.3.7.2 "AND" Logic

The "AND" logic is represented in Figure 1.3-26(b). Multiple input functions are required to produce an output function. In the "AND" logic, all input functions or a specified number of the input functions must be present to produce an output.

1.3.7.3 "NOT" Logic

The "NOT" logic represented in Figure 1.3-26(c) illustrates a function that will produce an output with no input signal. Likewise, with an input signal present, no output is produced.

1.3.7.4 Retentive Memory

This logic function in Figure 1.3-26(d) will either produce an output or not produce an output depending on its last energized input. If the lastinput signal received is the input aligned with the output, an output signal is allowed to pass. If the last input signal received is not aligned with the output, the output signal will be terminated.

1.3.7.5 Electrical Relay

Figure 1.3-27 illustrates the physical layout of a relay and the electrical circuit representations. There are two types of auxiliary contacts used in relays. The "A" contacts are shut when the main relay contacts are shut, and open when the main relay contacts are open. The "B" contacts are open when the main relay contacts are shut and shut when the main relay contacts are open. These "A" and "B" contacts are used as part of the instrumentation and control circuits for the system controlled by the relay.

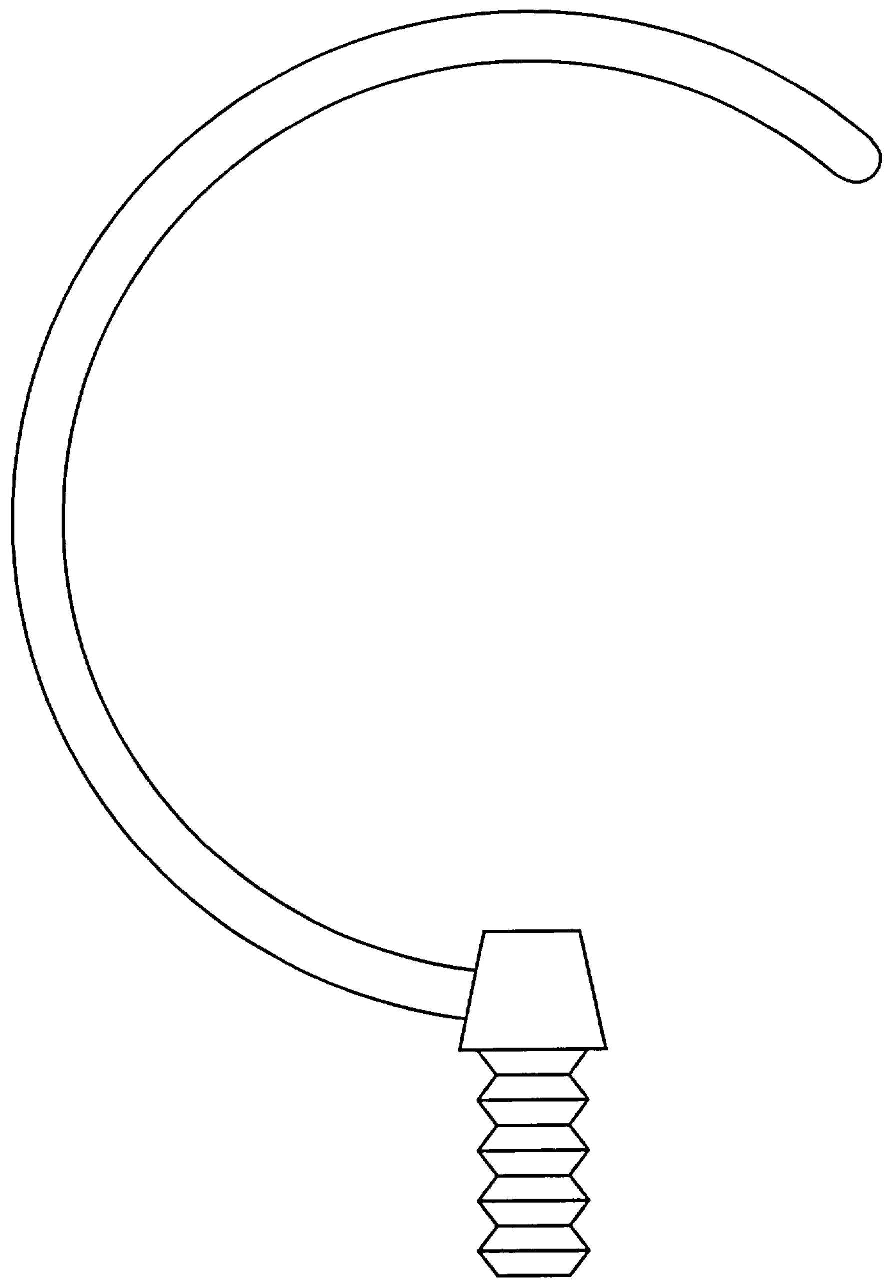
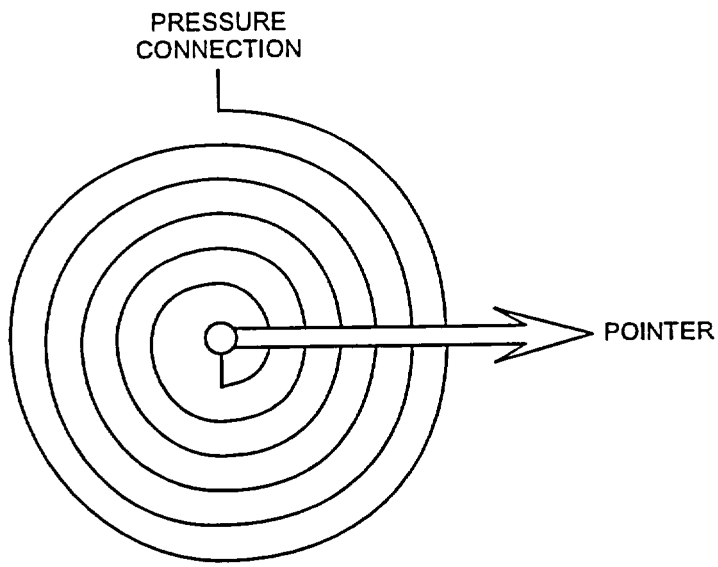
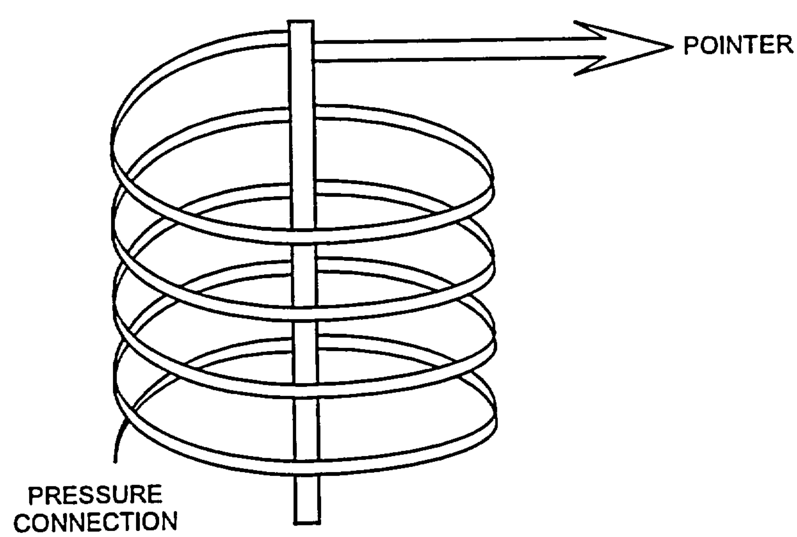


Figure 1.3-1 Simple Bourdon Tube

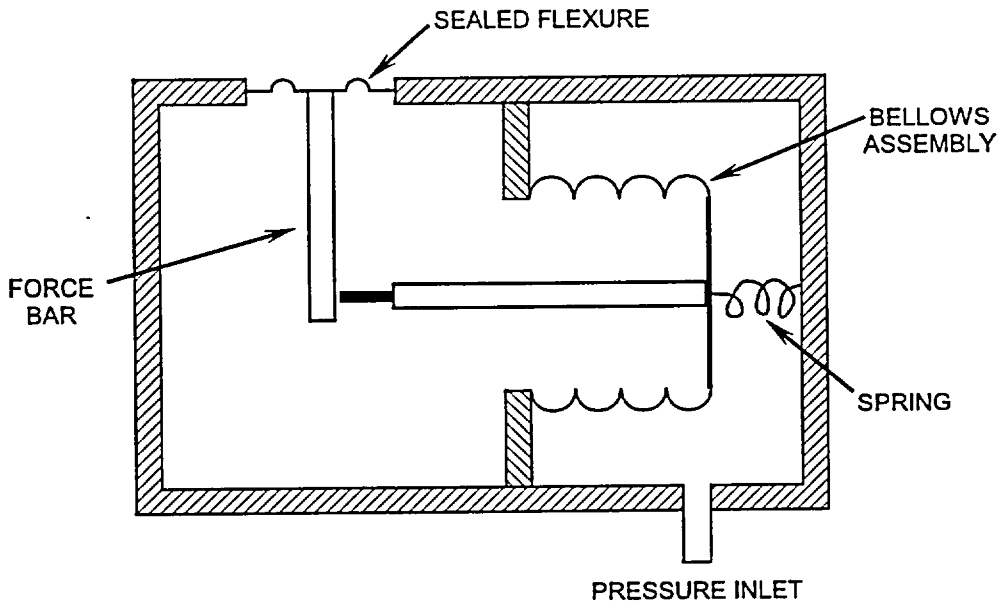


(a) Spiral pressure detector

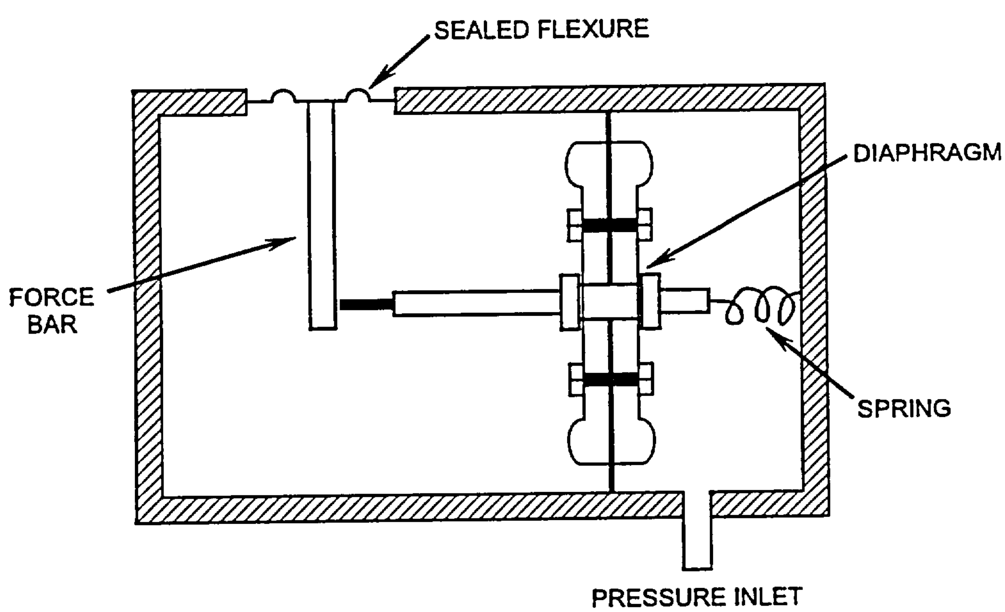


(b) Helical pressure detector

Figure 1.3-2 Wound Pressure Detectors



(b) Bellows Pressure Sensor



(b) Diaphragm Pressure Sensor

Figure 1.3-3 Sealed Pressure Detectors

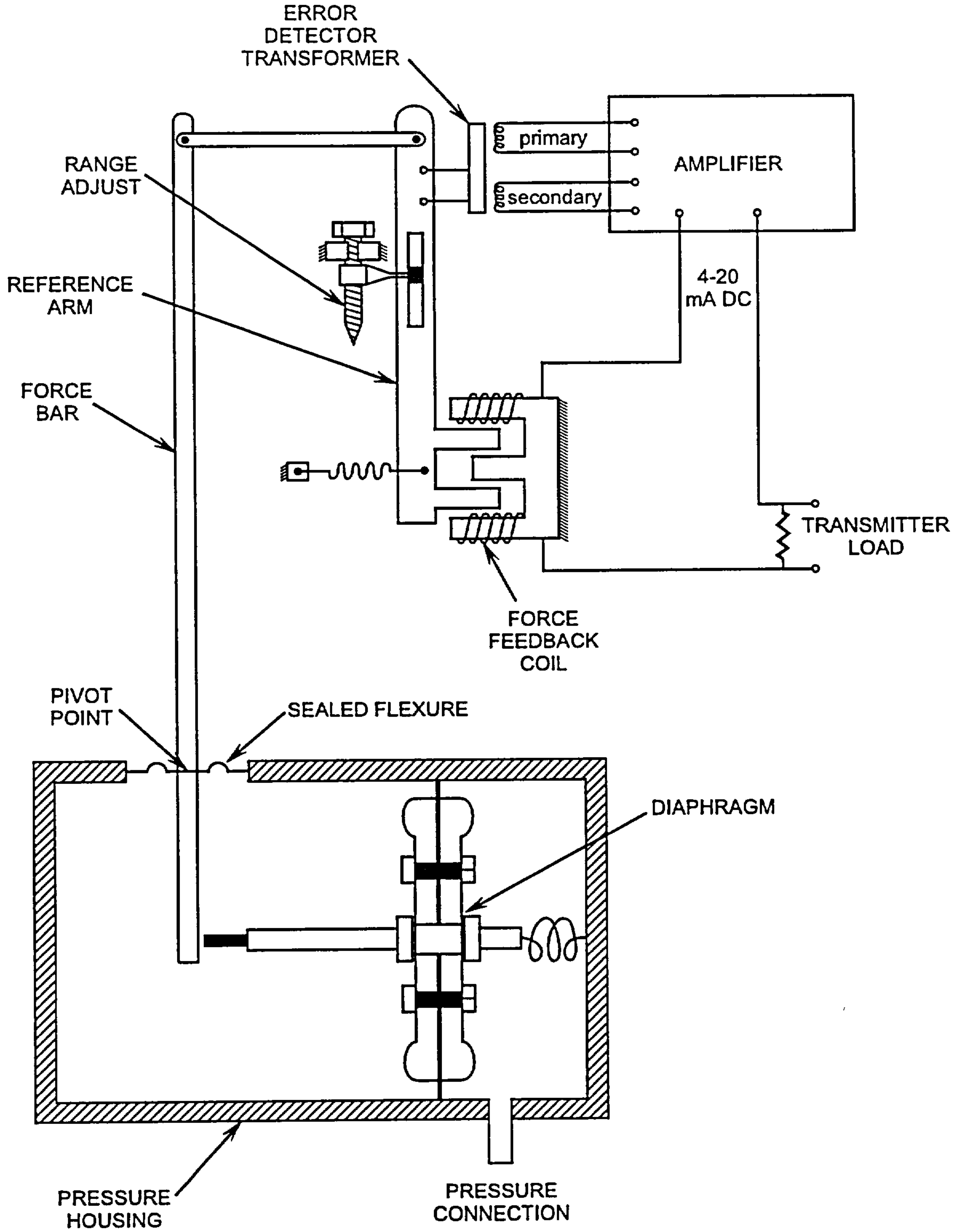
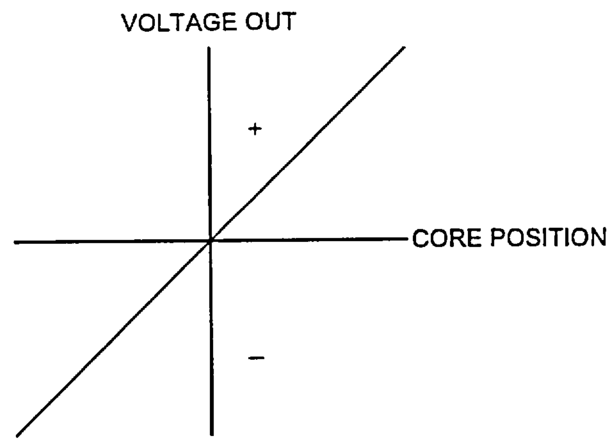


Figure 1.3-4 Force Balance Transmitters



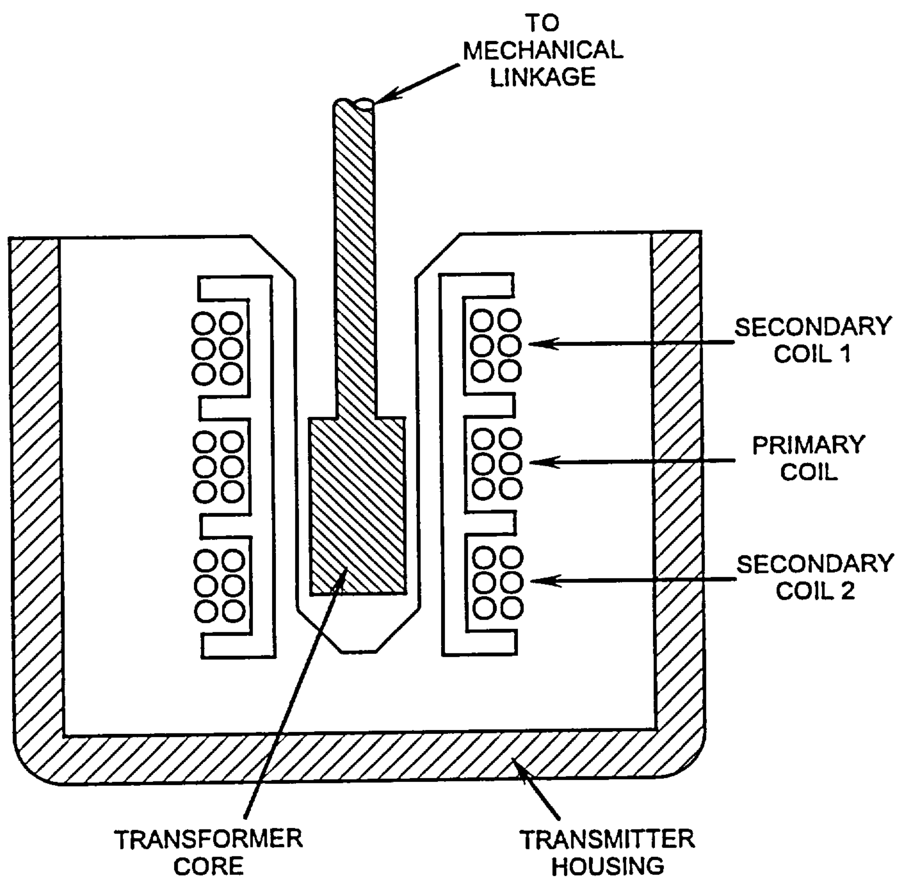


Figure 1.3-5 Movable Core Transmitters

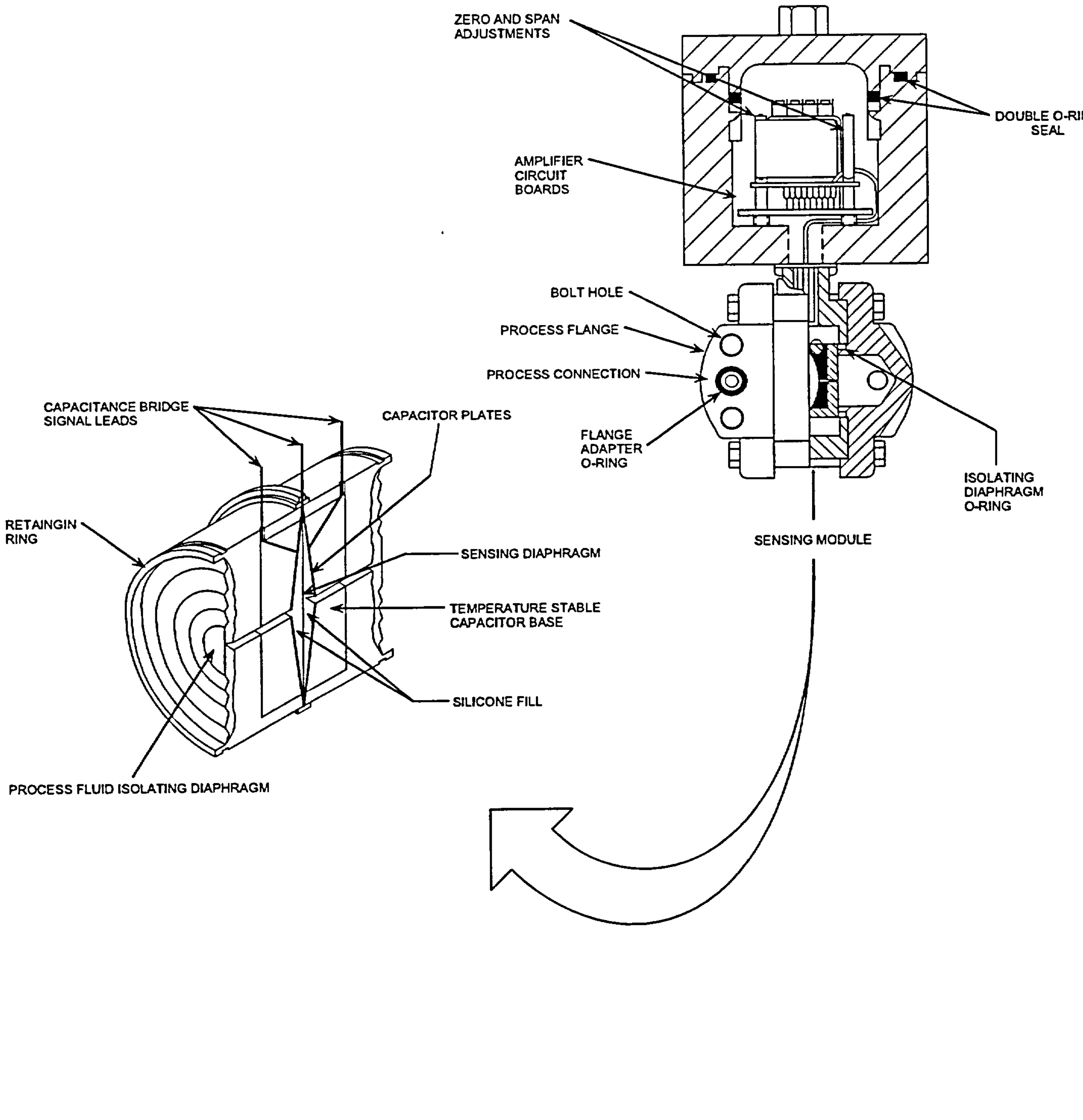


Figure 1.3-6 Variable Capacitance Transmitters

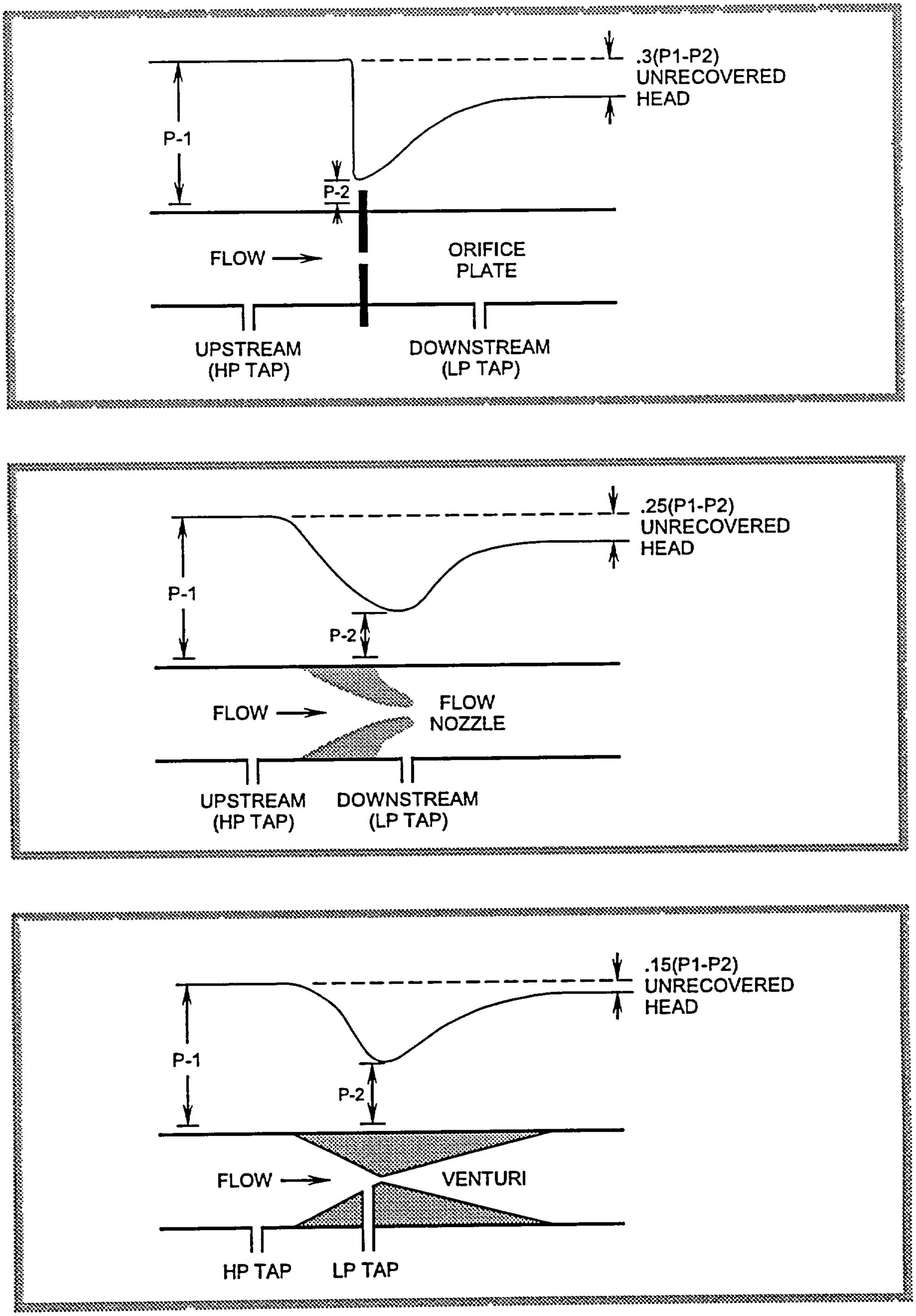


Figure 1.3-7 Primary Devices

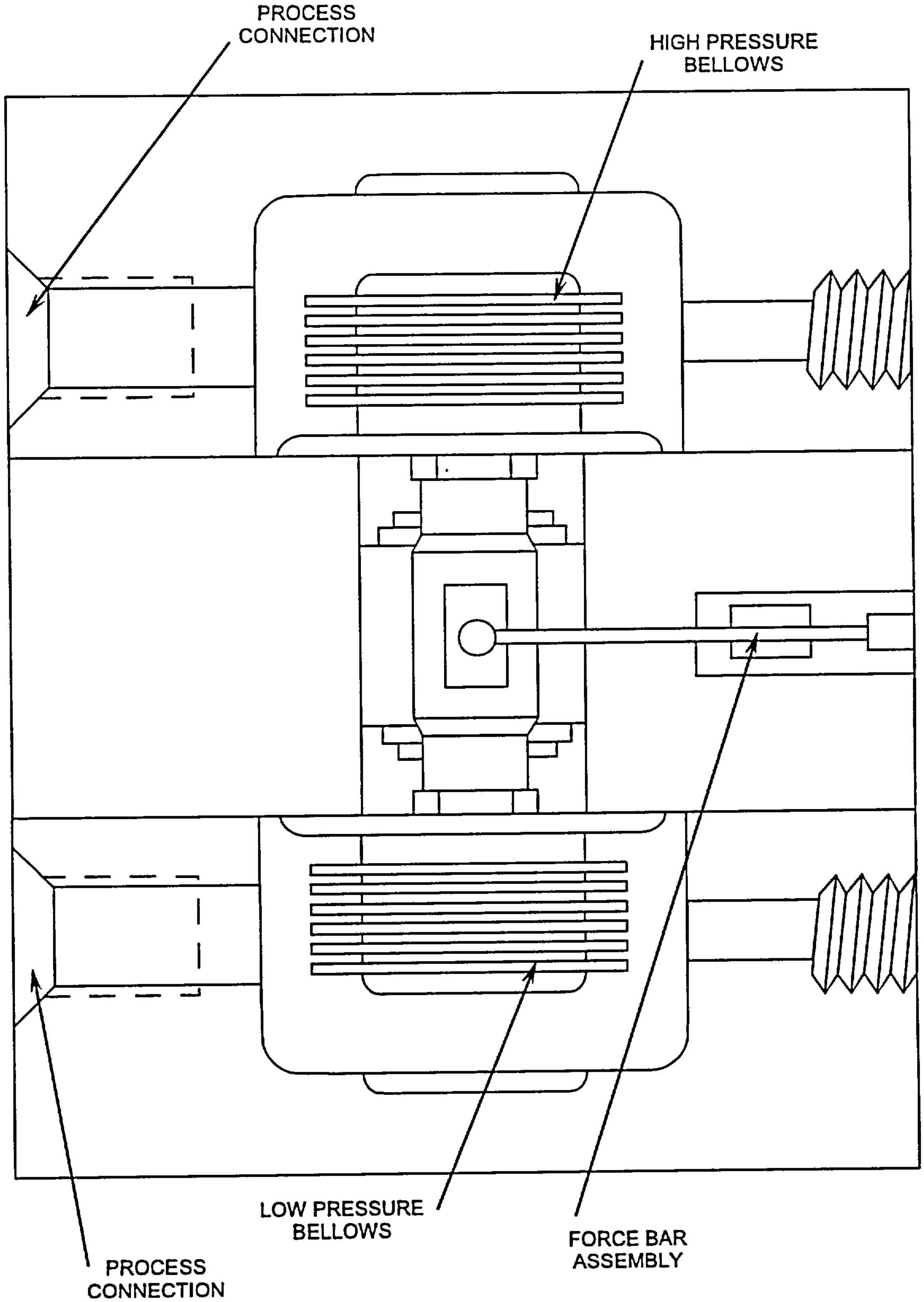


Figure 1.3-8 Bellows Flow Sensor

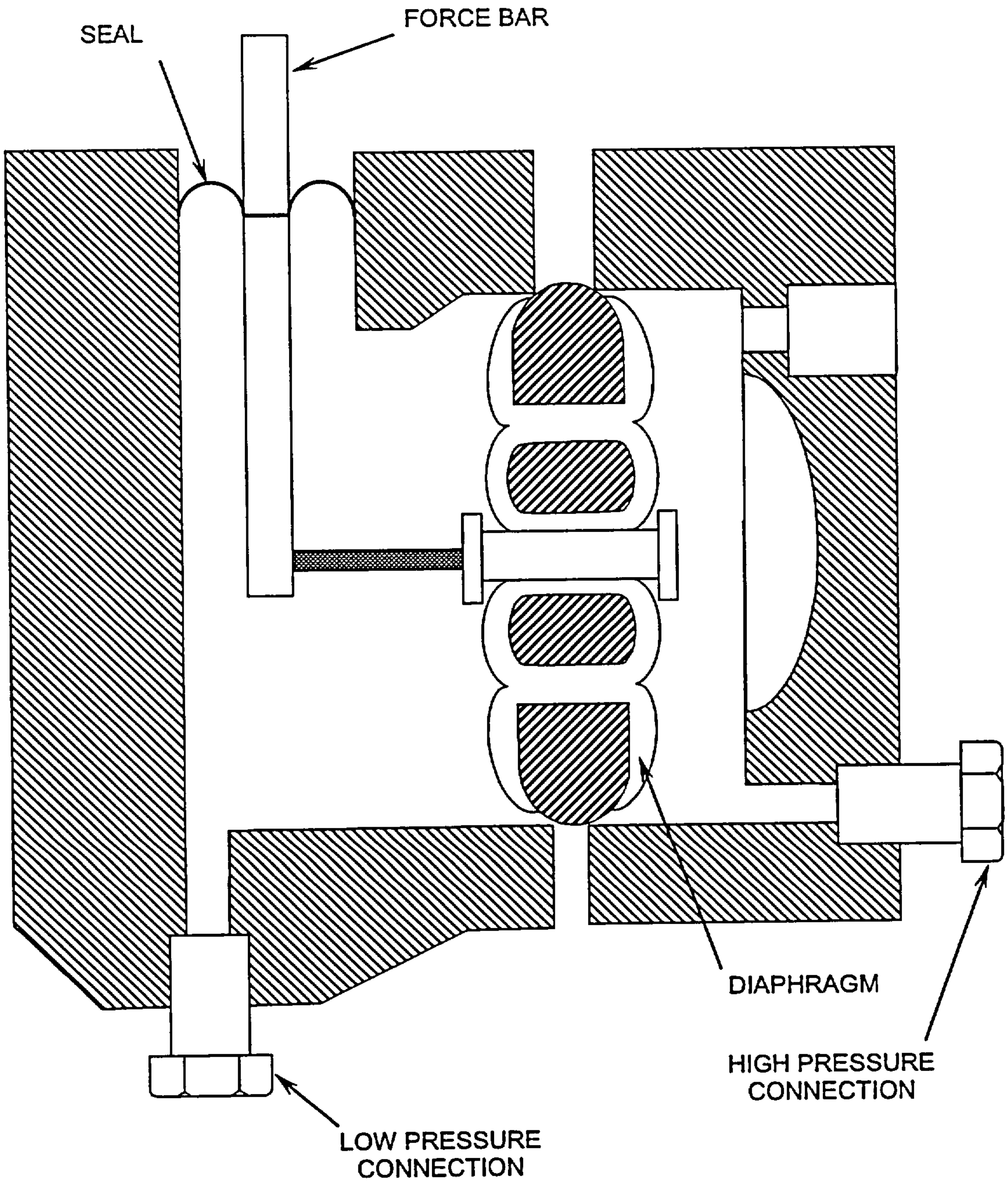


Figure 1.3-9 Diaphragm Flow Sensor

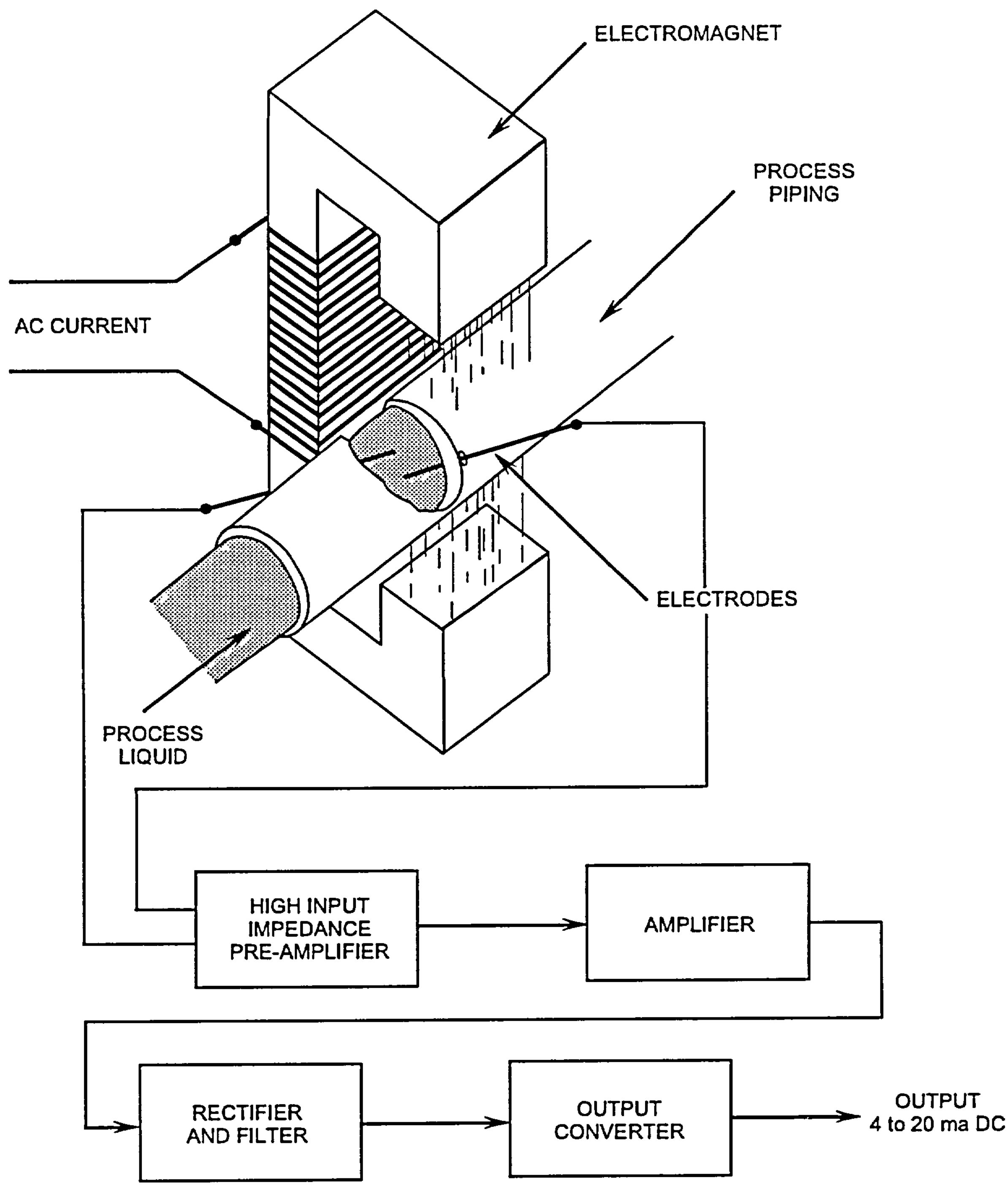


Figure 1.3-10 Magnetic Flow Meter

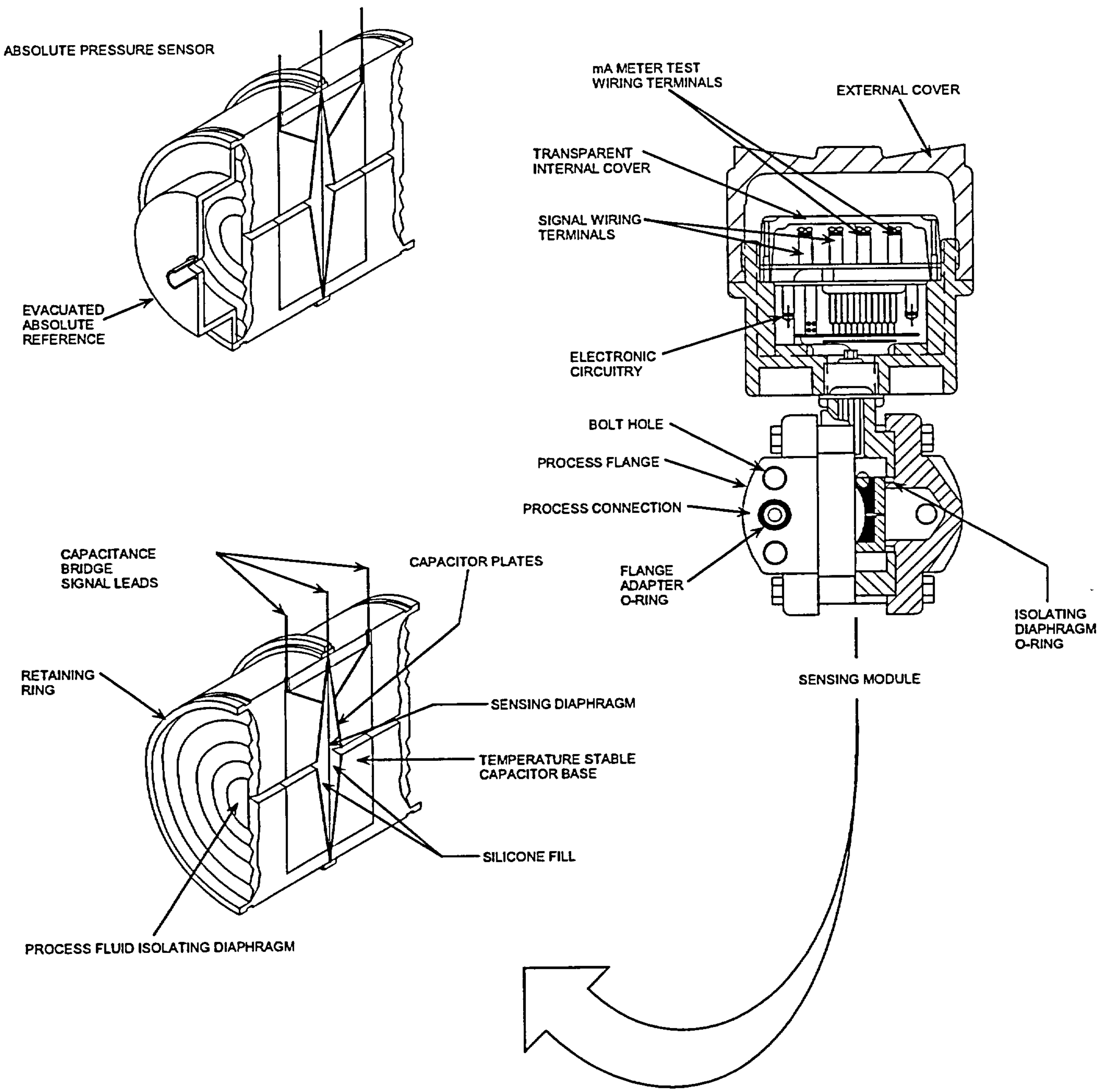


Figure 1.3-11 Variable Capacitance Differential Pressure Sensor

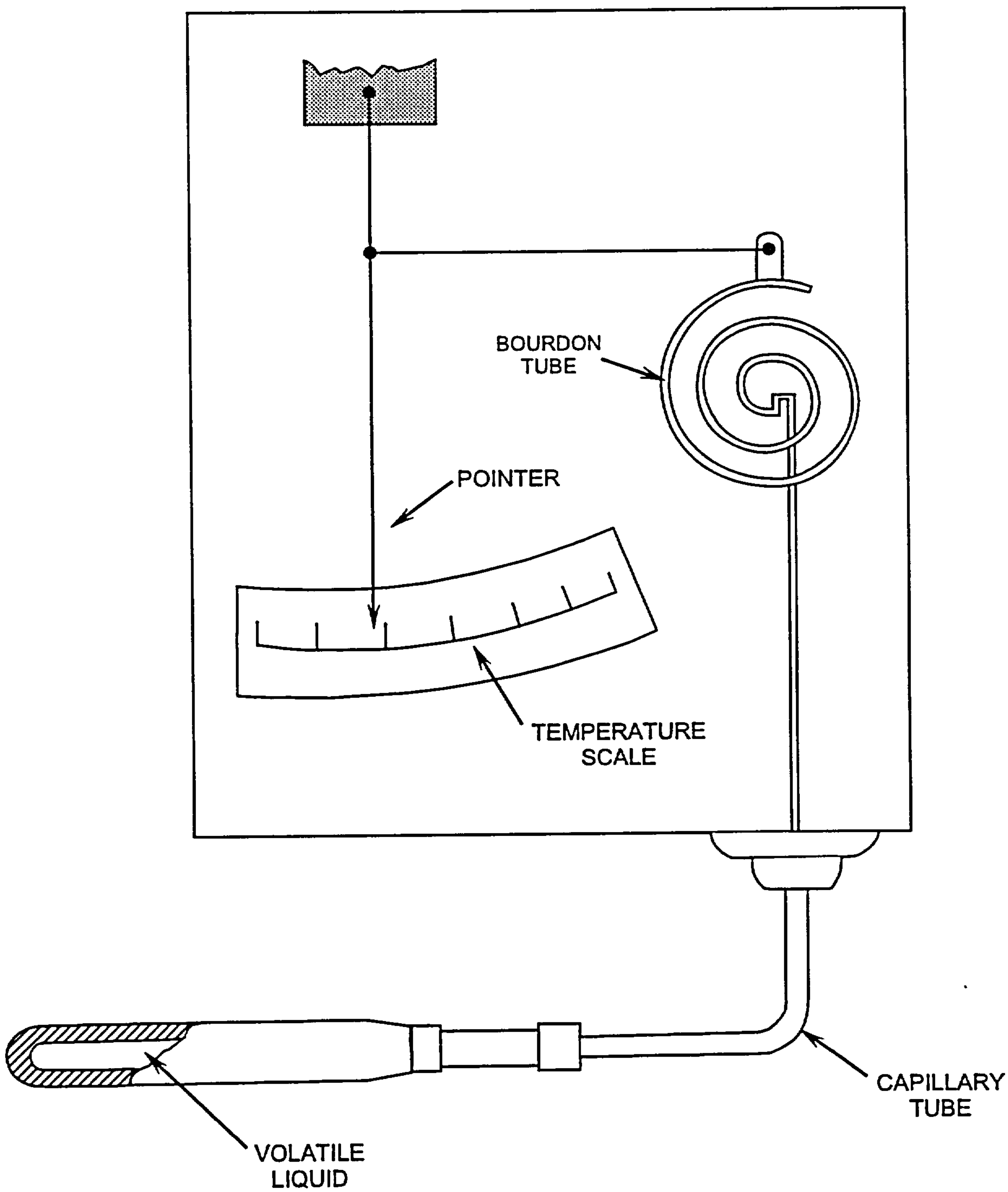


Figure 1.3-12 Fluid Filled Temperature Sensor

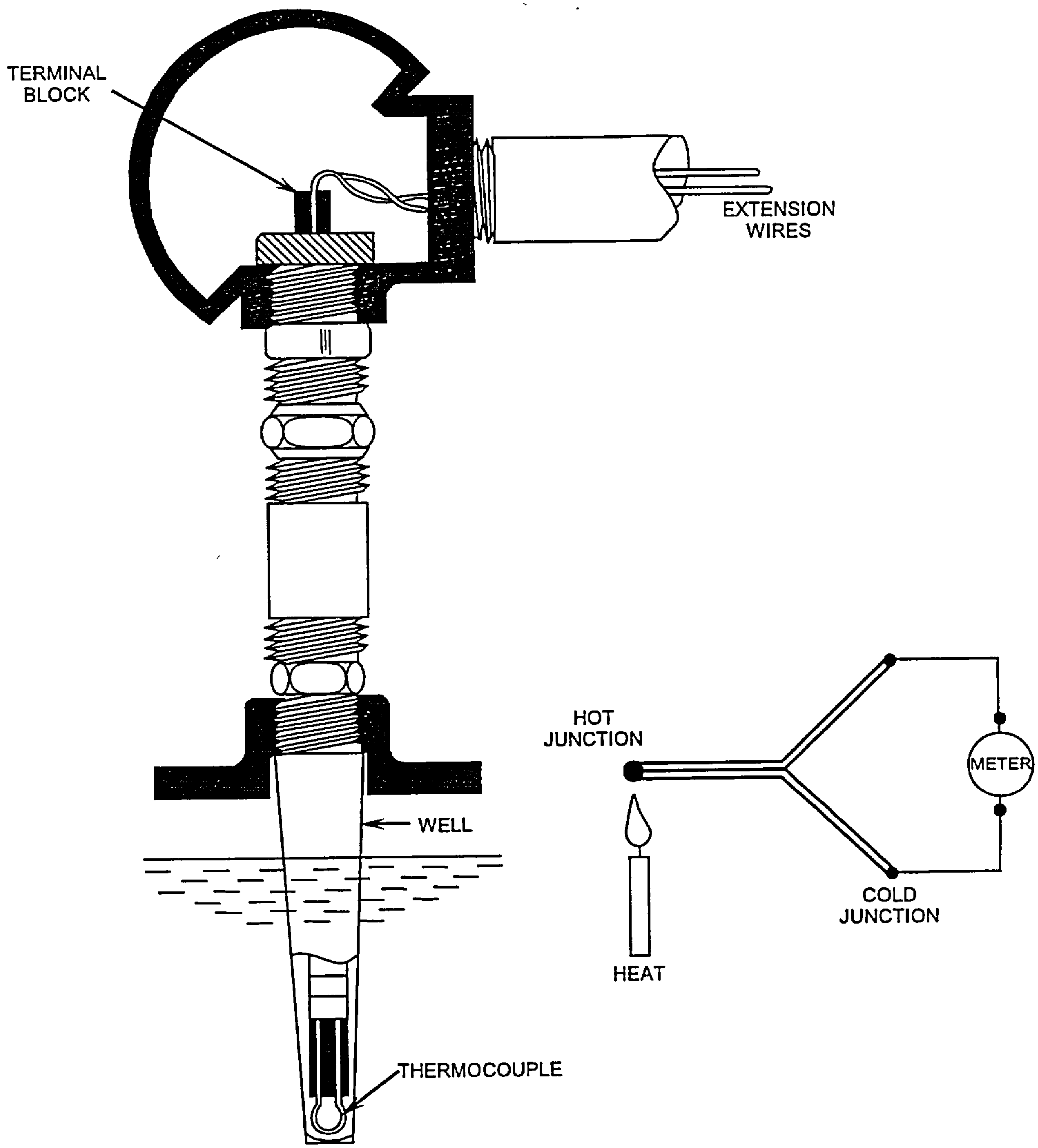


Figure 1.3-13 Thermocouple

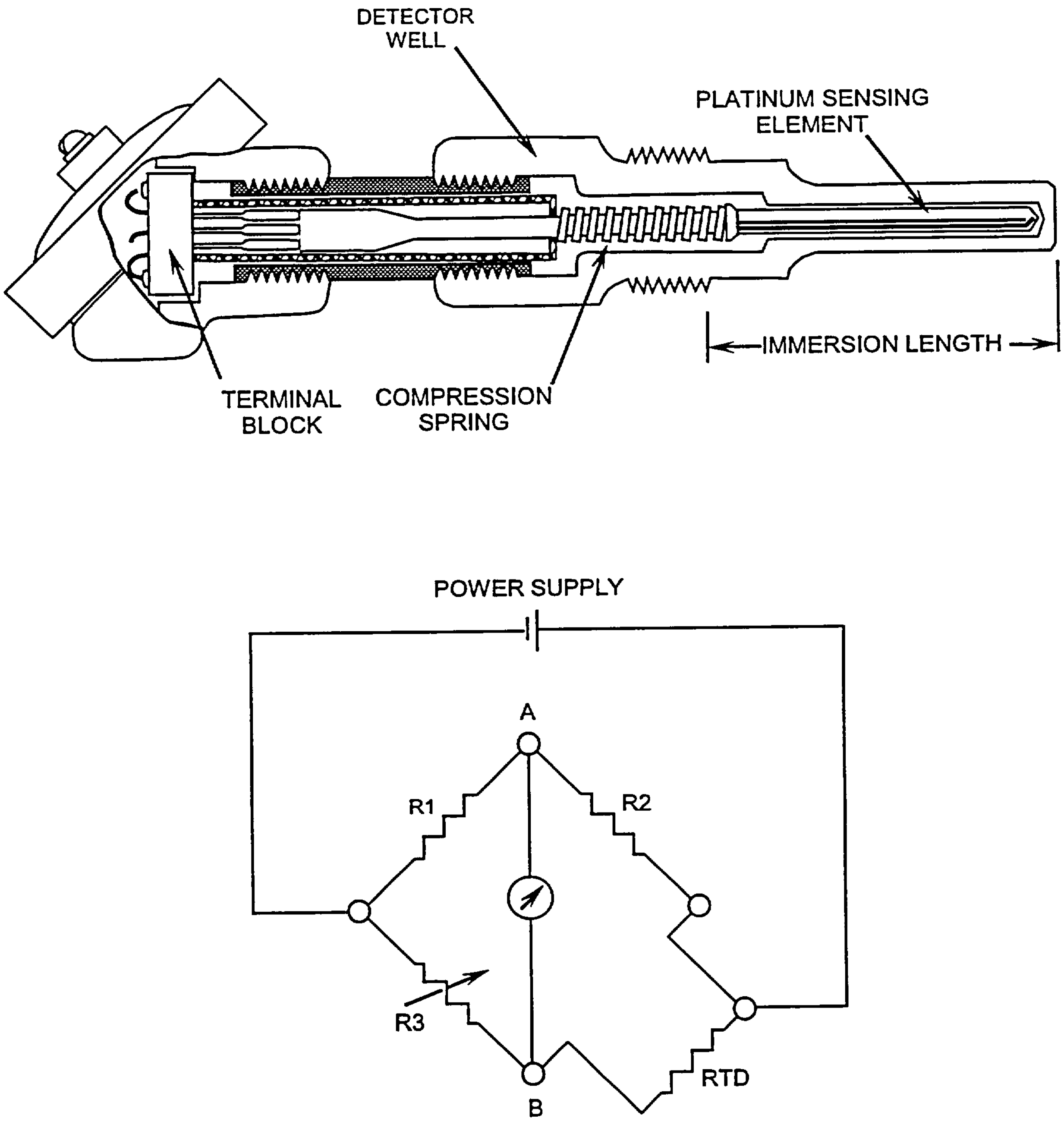


Figure 1.3-14 Resistance Temperature Detector

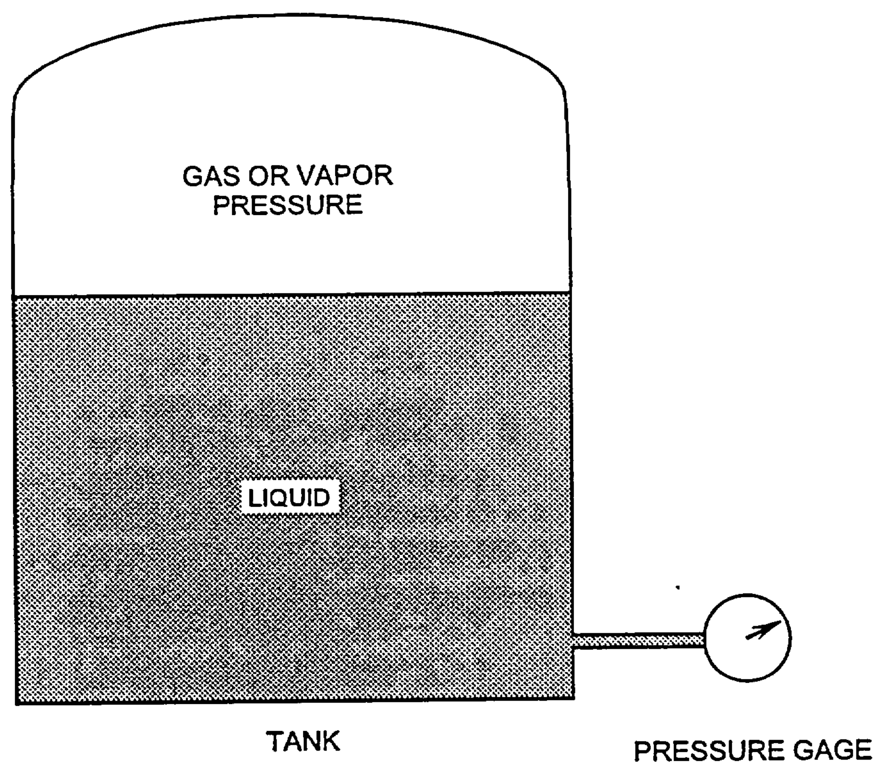


Figure 1.3-15 Direct Level Measure Devices

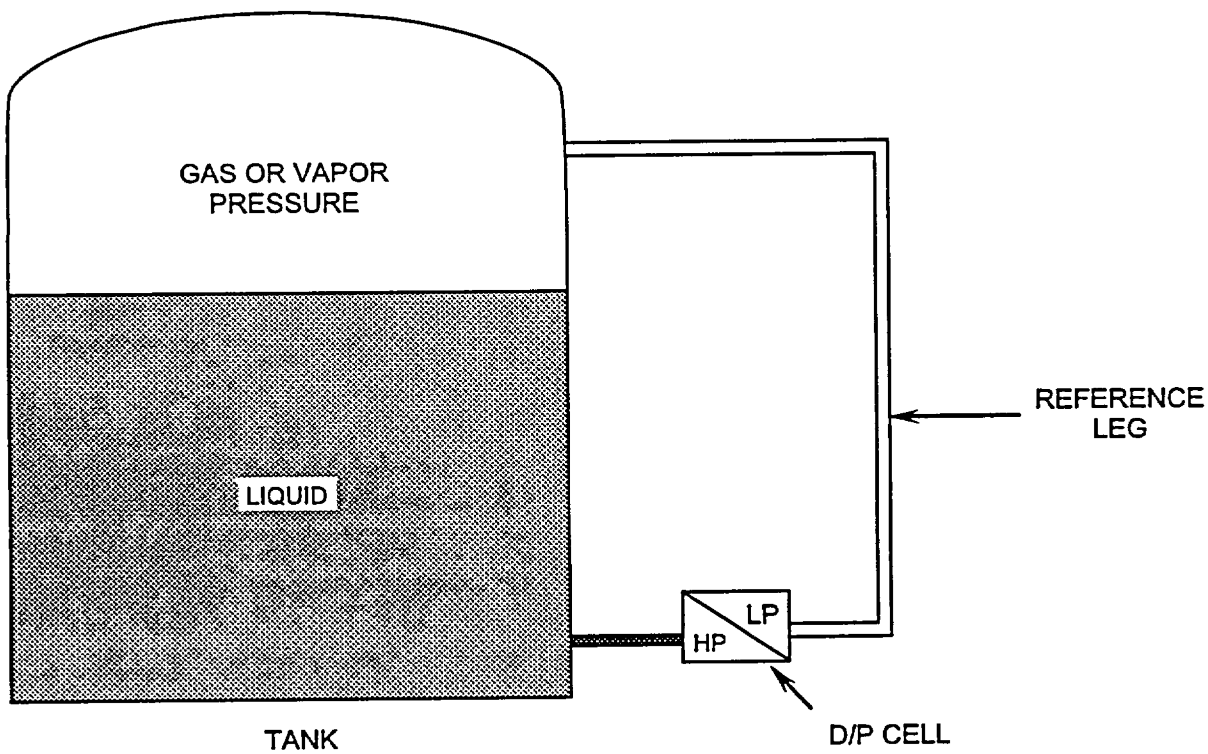


Figure 1.3-16 Differential Pressure Level Detector

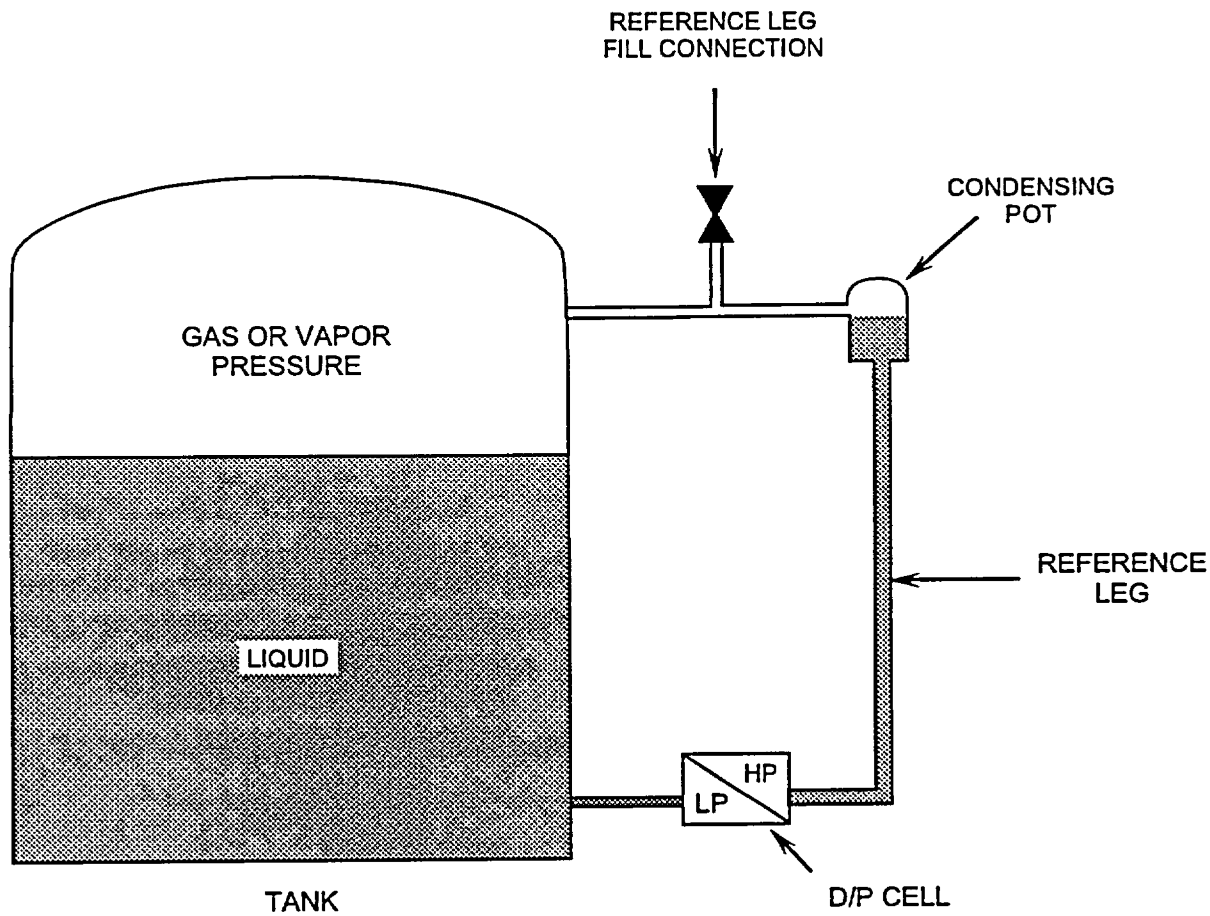


Figure 1.3-17 Reference Leg Differential Pressure System

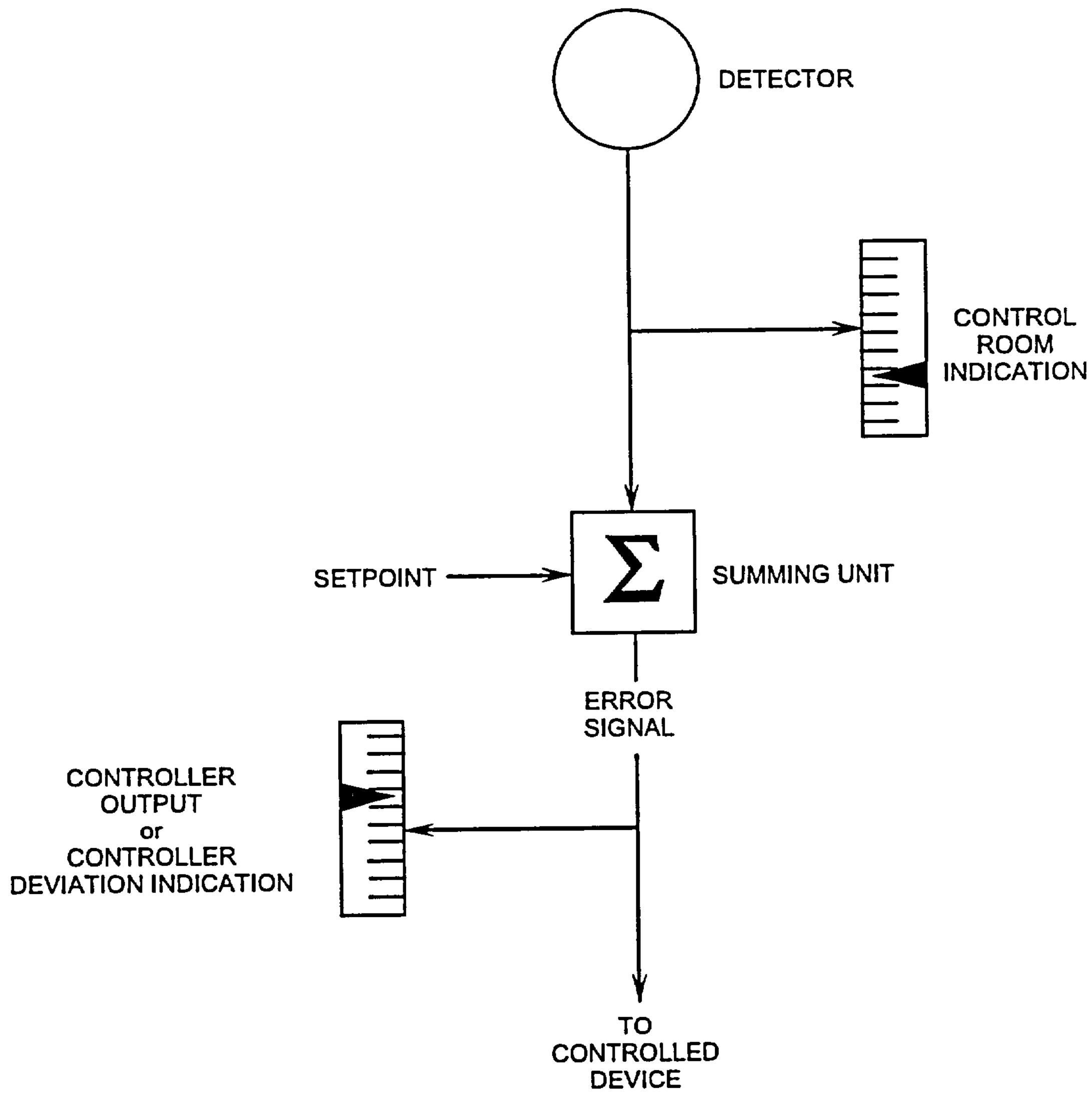


Figure 1.3-18 Basic Control Diagram

0199-1

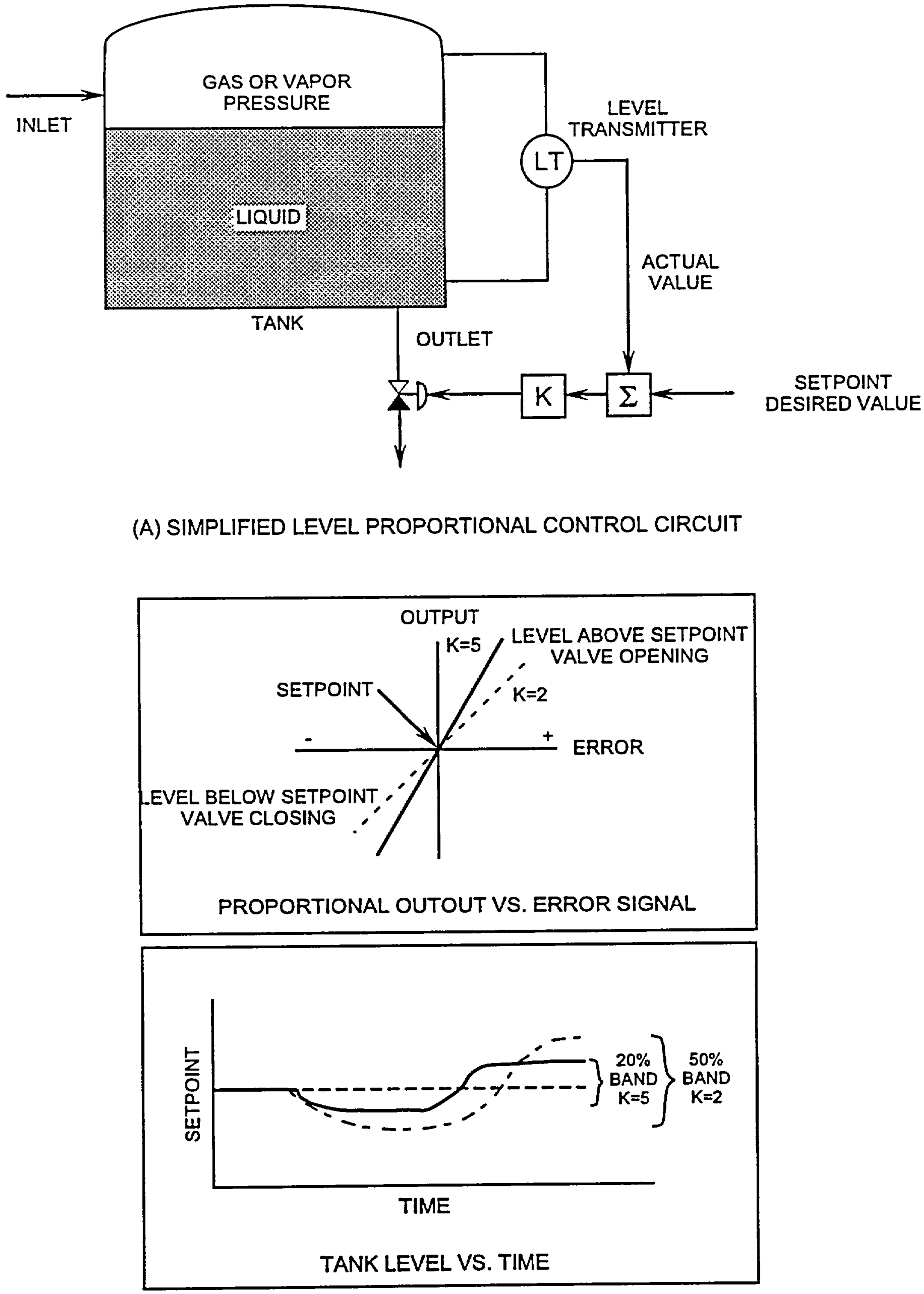
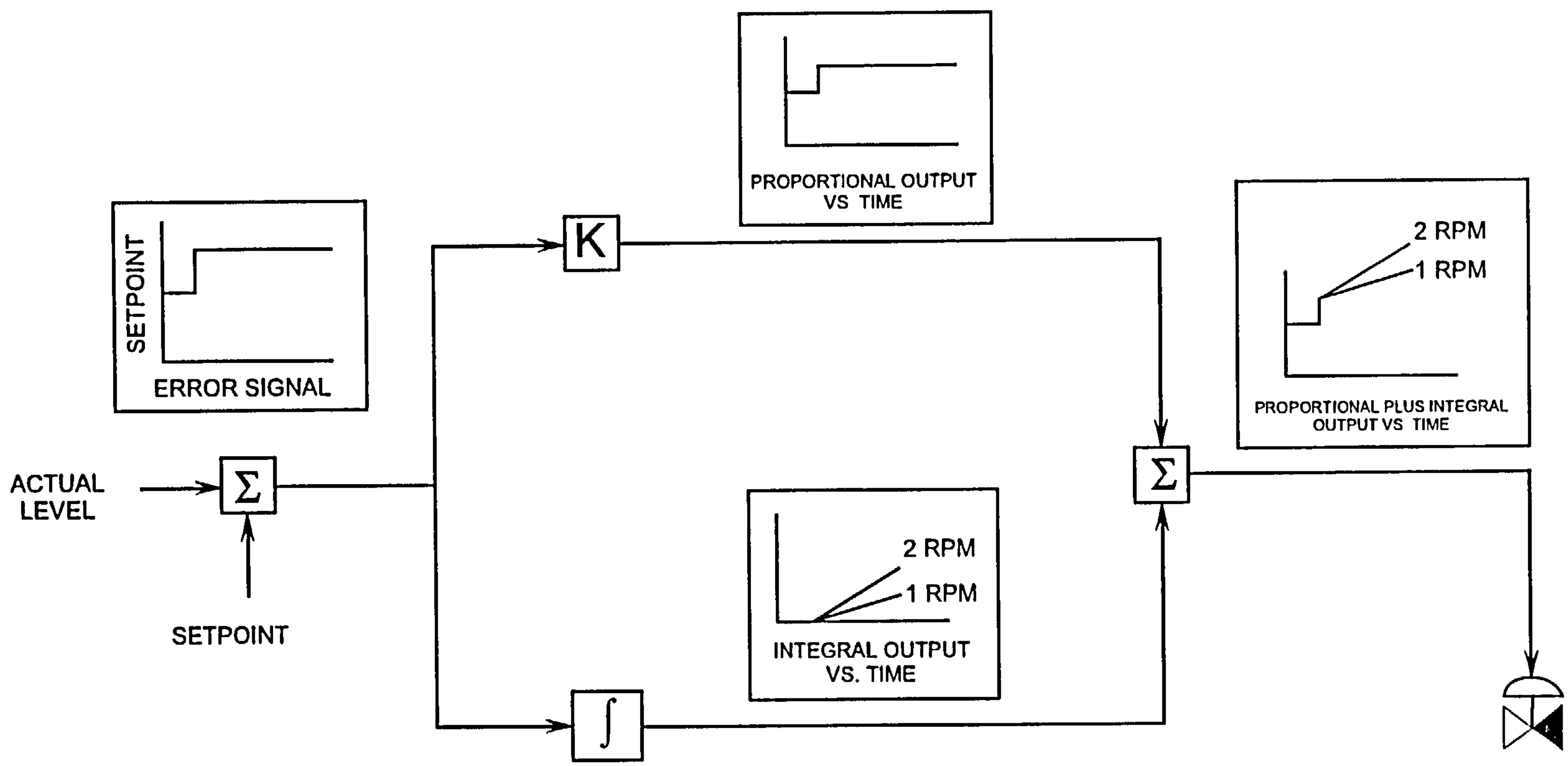


Figure 1.3-19 Proportional Controller



PROPORTIONAL PLUS INTEGRAL CONTROL CIRCUIT

Figure 1.3-20 Proportional Plus Integral Controller

0199-1

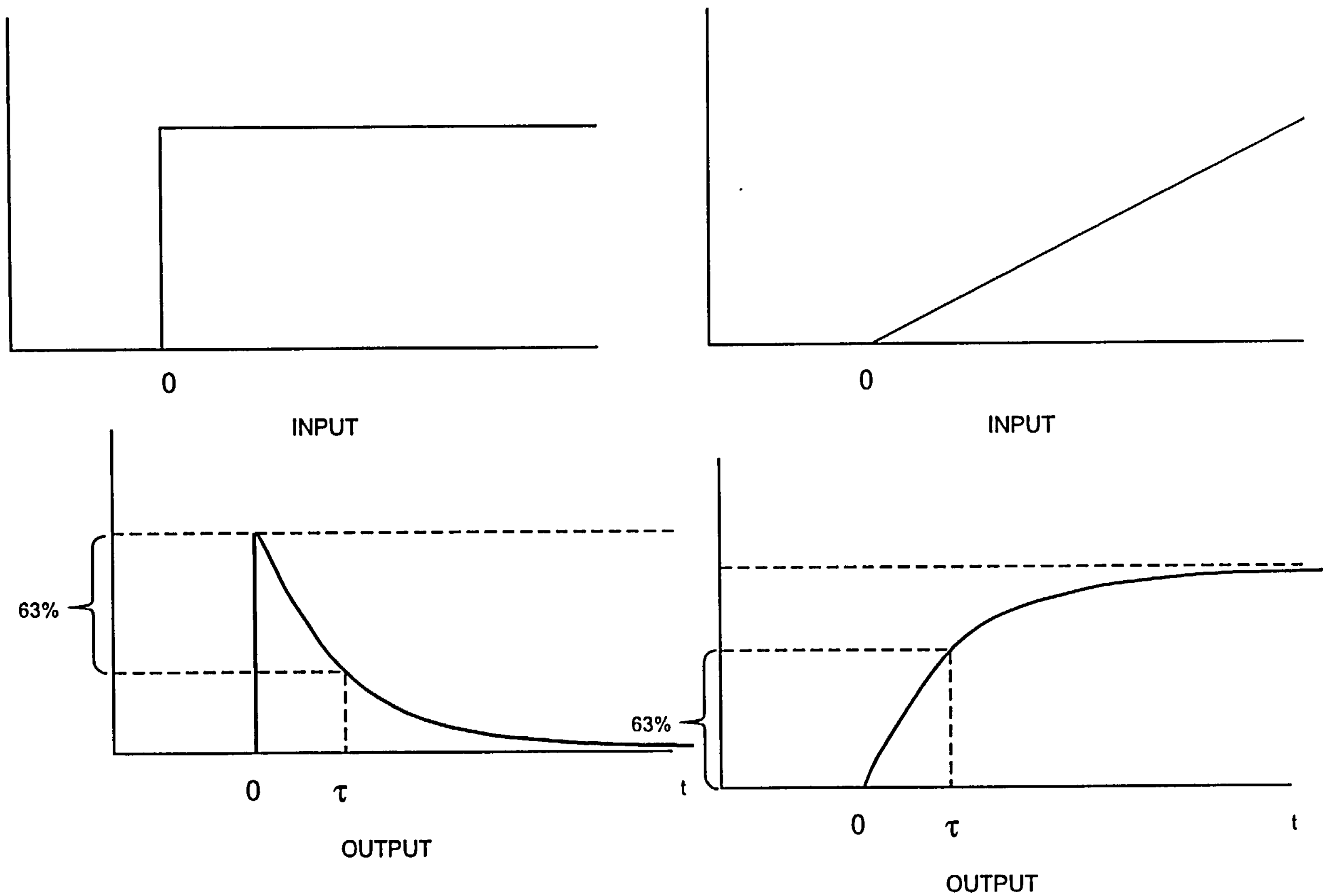
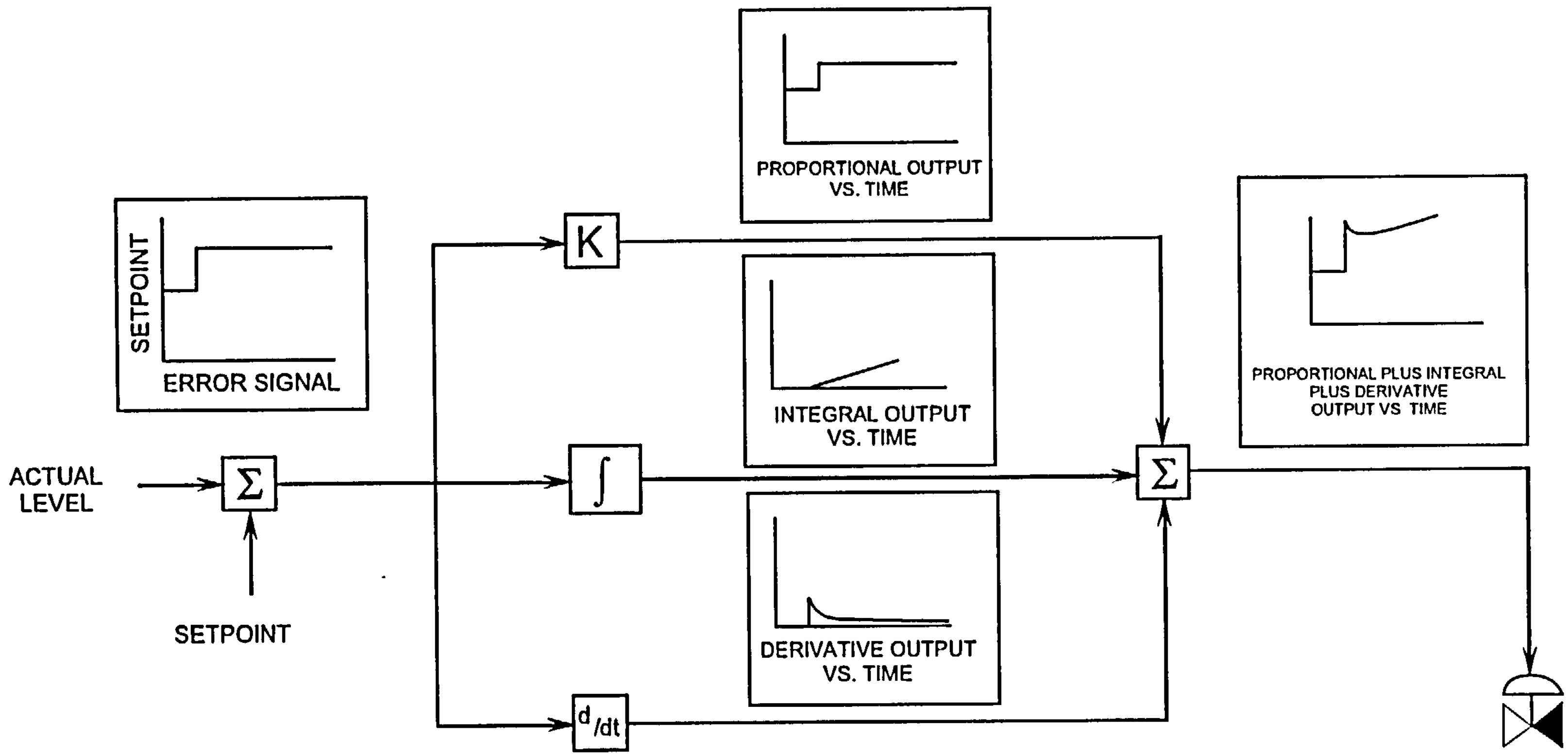


Figure 1.3-21 Time Constant

0199-1



PROPORTIONAL PLUS INTEGRAL PLUS DERIVATIVE CONTROL CIRCUIT

Figure 1.3-22 Proportional Plus Integral Plus Derivative Controller

0199-1

0199-1

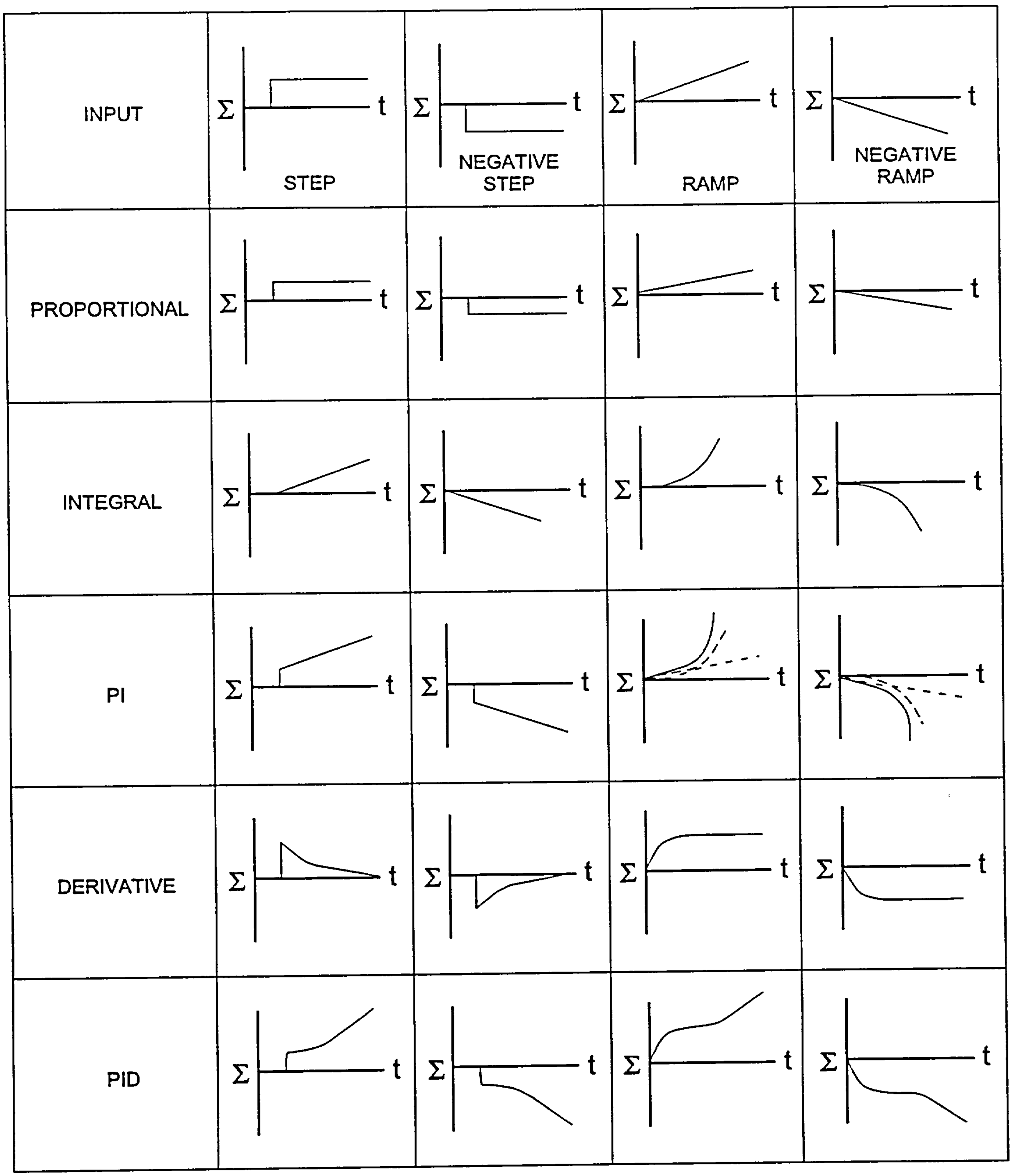


Figure 1.3-23 PID Controller Responses

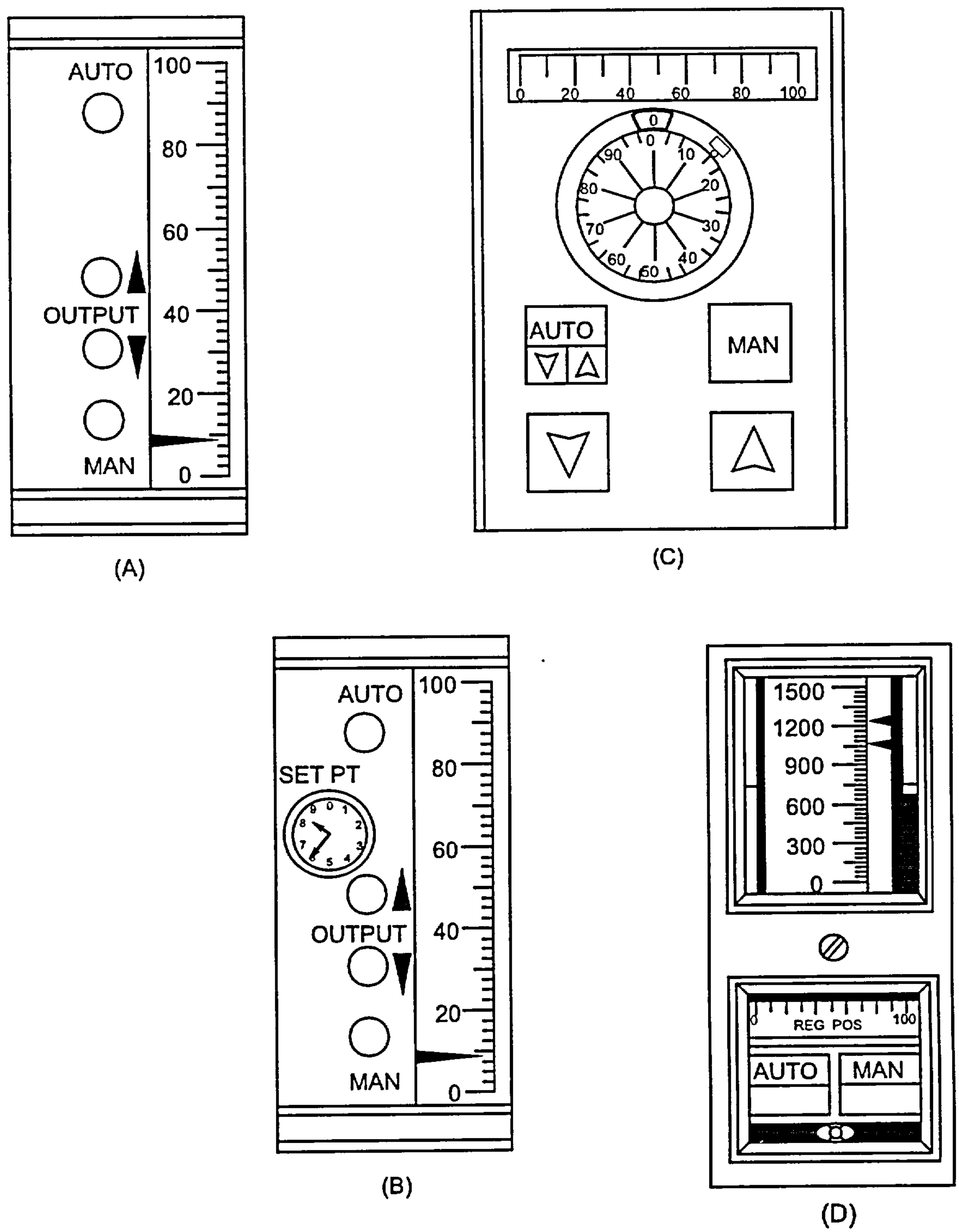


Figure 1.3-24 Manual/Auto Control Stations

0199-1

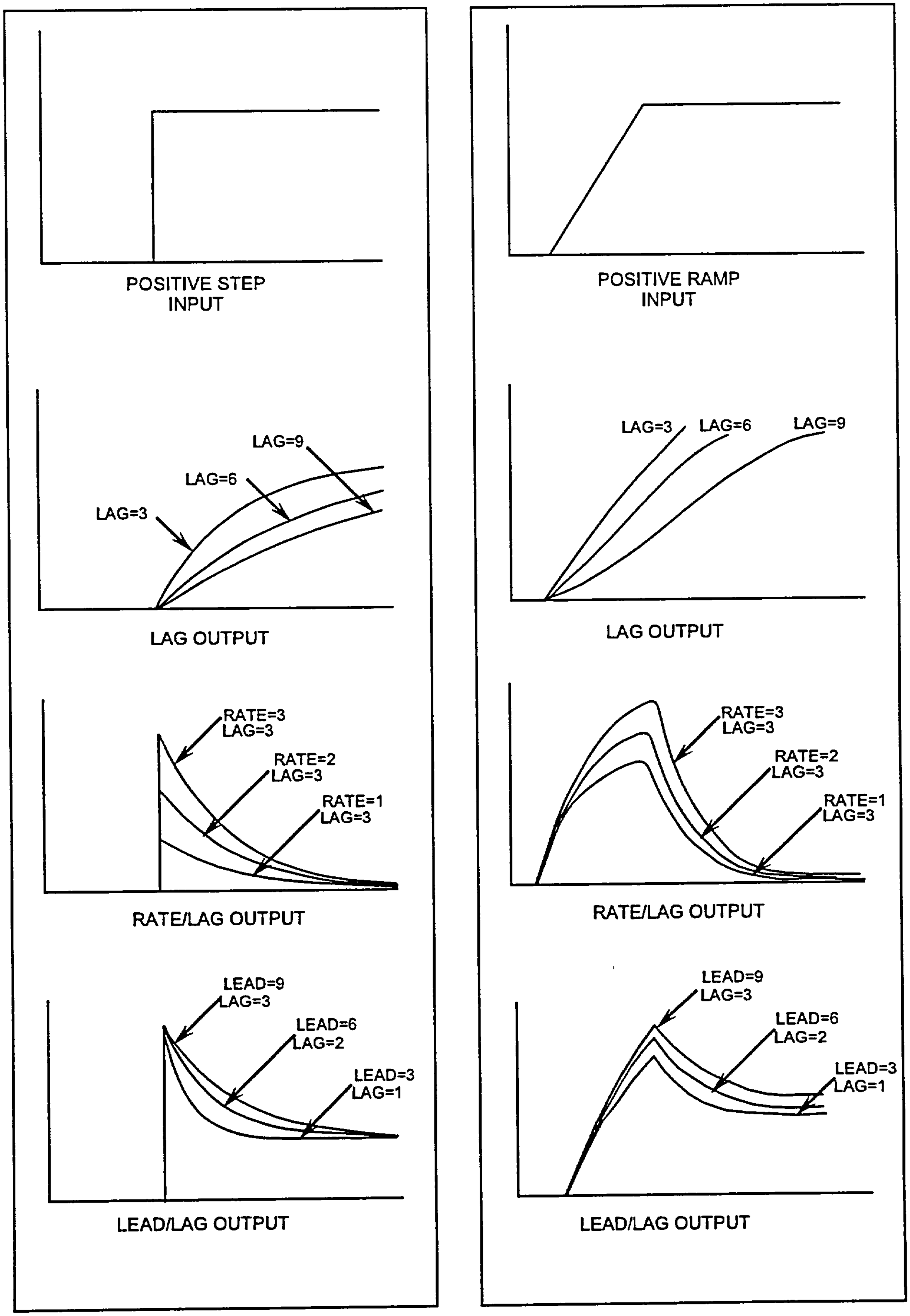


Figure 1.3-25 Signal Conditioning Output with Varying Time Constants

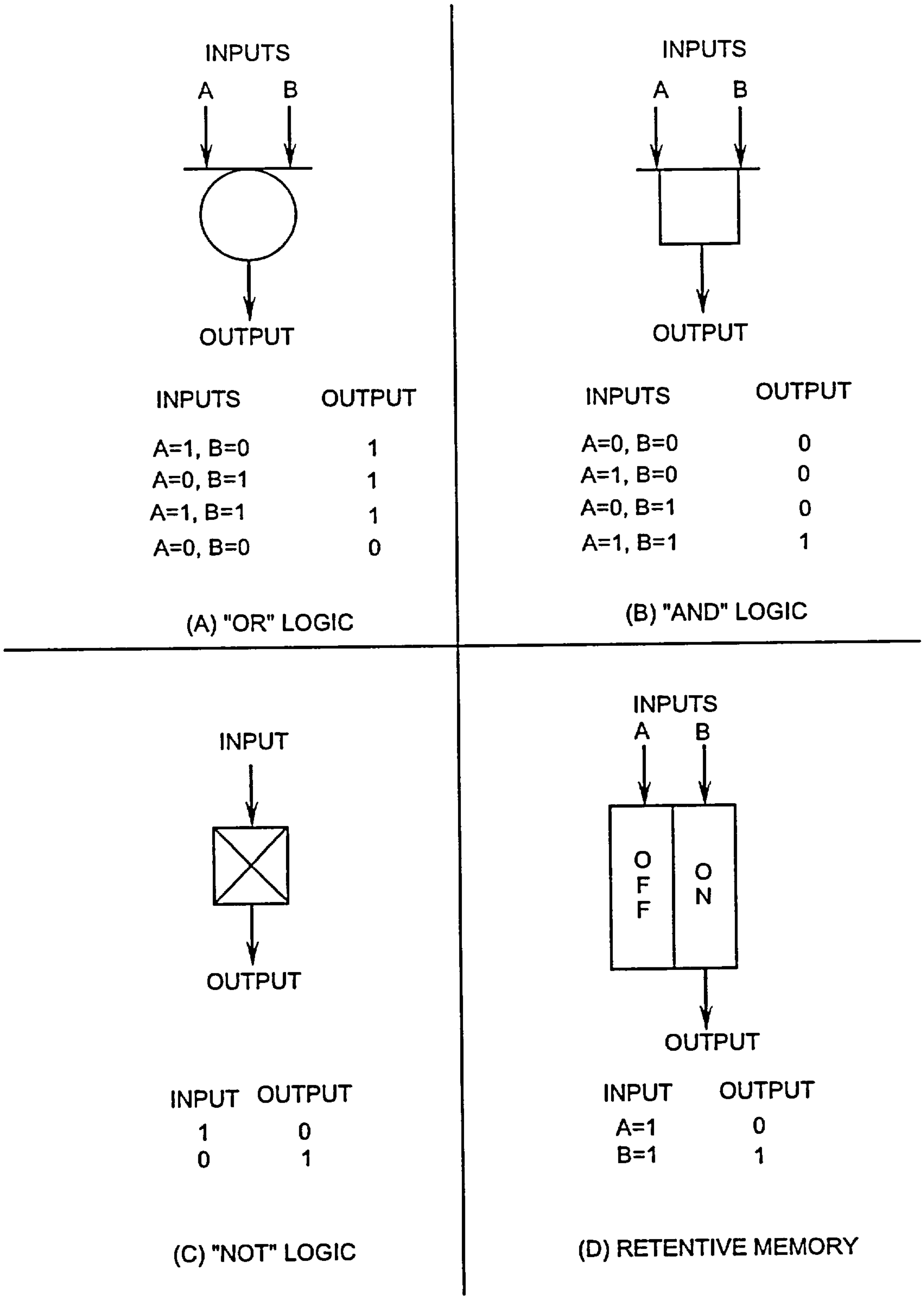
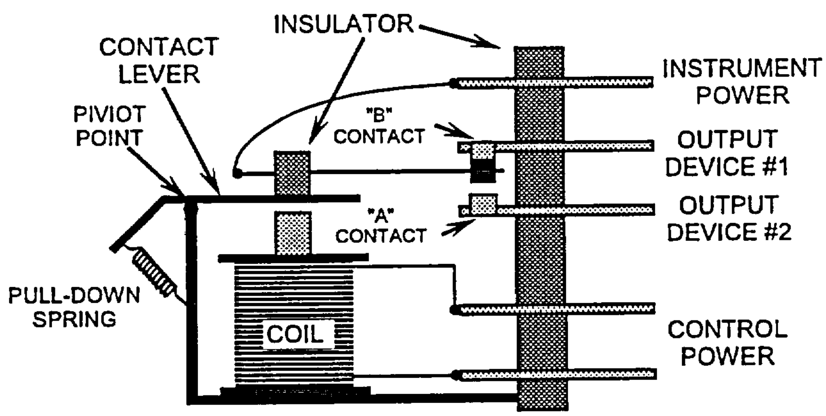
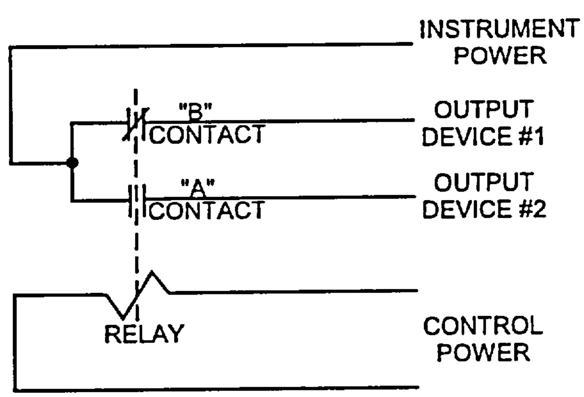


Figure 1.3-26 Logic Functions



RELAY - MECHANICAL OPERATION

RELAY SHOWN DE-ENERGIZED



RELAY - ELECTRICAL OPERATION

RELAY SHOWN DE-ENERGIZED

Figure 1.3-27 Relay

Westinghouse Technology Systems Manual

Section 1.4

Introduction to Probabilistic Risk Assessment

TABLE OF CONTENTS

LIST OF FIGURES

1.4 INTRODUCTION TO PROBABILISTIC RISK ASSESSMENT

Learning Objectives:

1. Define the term risk.
2. List the three questions that a plant PRA answers.
3. Describe the different levels of PRA.
4. Define the terms: internal and external initiating event, accident sequence, plant damage state, front-line system, and support system.
5. Explain why event tree analysis is performed and the important features of an event tree.
6. Explain why fault tree analysis is performed and the four types of faults included in the fault trees.
7. List the four types of accident sequences that are important.
8. Identify how importance measures can be used in risk management.
9. List three regulatory uses of PRA.
10. List two utility uses of PRA.
11. Identify two possible uses of PRA information for plant inspectors.

1.4.1 Introduction

There are many definitions of risk. However, most of them include two basic factors: likelihood and consequences. Therefore, for the purpose of nuclear power plant safety assessments, risk is defined as the likelihood and consequences of potential accidents at commercial nuclear power plants.

A Probabilistic Risk Assessment (PRA) is an engineering tool used to quantify the risk of a facility. PRA is used primarily to address the likelihood and consequences of rare events at nuclear power plants. These events are generally referred to as severe accidents. The PRA augments traditional engineering analyses by providing quantitative measures of safety and thus a means of addressing the relative significance of issues in relation to plant safety. Basically, a nuclear power plant PRA answers three questions:

- What can go wrong?
- How likely is it?
- What are the consequences?

Probabilistic risk assessment is a multi-disciplinary approach employing various methods including system reliability, containment response, and fission release and public consequence analyses. PRA treats the entire plant and its constituent systems in an integrated fashion. Because of this, subtle interrelationships can be discovered that are important to risk. Another important attribute of the PRA method is it involves both single and multiple failure analysis. Multiple failures often lead to situations beyond system design basis and, in some cases, are more likely than single failures. By addressing multiple failures, the PRA can cover a broad spectrum of potential accidents at plants.

1.4.2 History and Background

The first comprehensive development and application of PRA techniques in the commercial nuclear power industry was the NRC sponsored Reactor Safety Study (RSS). The RSS analyzed both a BWR (Peach Bottom) and PWR (Surry). The report of the RSS results (1), generally referred to as WASH-1400, was published in

October of 1975. The basic PRA approach developed by the RSS is still used today.

The principal objective of the RSS was to quantify the risk to the public from U.S. commercial nuclear power plants. Because it was the first broad scale application of event and fault tree methods to a system as complex as a nuclear power plant; analyzed conditions beyond the design basis; and attempted to quantify the risk; it was one of the more controversial documents in the history of reactor safety.

A group called the Lewis Committee performed a peer review on the RSS and published a report (2), NUREG/CR-0400, to the U.S. Nuclear Regulatory Commission three years later to describe the effect of the RSS results on the regulatory process. The report concluded that although the RSS had some flaws and PRA had not been formally used in the licensing process, PRA methods were the best available and should be used to assist in the allocation of the limited resources available for the improvement of safety.

The 1979 accident at Three Mile Island (TMI) substantially changed the character of the NRC's regulatory system. The accident revealed that perhaps nuclear reactors might not be safe enough and that new policies and approaches were required. Based on comments and recommendation from the Kemeny and Rogovin investigations (3) of the TMI accident, a substantial research program on severe accident phenomenology was initiated (e.g., those accidents beyond the design basis which could result in core damage). It was also recommended that PRA be used more by the staff to complement its traditional, non-probabilistic methods of analyzing nuclear plant safety. Rogovin also suggested in a report (4) to the Commissioners and the public, NUREG/CR-1250, that the NRC policy on severe accidents consider 1) more severe accidents in the licensing process and 2) probabilistic safety goals to help define what is an acceptable level of plant safety.

Soon thereafter, the NRC staff sponsored the Interim Reliability Evaluation Program (5), a series of plant reliability studies reported in NUREG/CR-2728, to develop methods for the efficient use of PRA to analyze the various designs of operating reactors and to increase the cadre of experienced PRA practitioners. By the mid 1980's, general procedures for performing PRAs were developed and documented in the PRA Procedures Guide (6), NUREG/CR-2300. The current status of PRA, its relationship to the nuclear regulatory process, and a summary of PRA perspectives available at that time (1984) was published in the Probabilistic Risk Assessment Reference Document (7), NUREG-1050. This document also discussed the potential uses of PRA results for regulatory purposes.

In the late 1980, the U.S. Nuclear Regulatory Commission sponsored a current assessment of severe accident risks for five commercial nuclear power plants in a report called Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants (8), NUREG-1150. This report included an update of the RSS risk assessments of Surry and Peach Bottom and provided the latest NRC version of the state of the art in PRA models, methods, and approaches. The results were to be used to support prioritization of safety issues.

Recently, the NRC issued a letter to initiate an Individual Plant Examination (IPE) Program for Severe Accident Vulnerabilities (9), Generic Letter No. 88-20. The NRC requested each licensed nuclear power plant to identify plant specific vulnerabilities to severe accidents by performance of a Level 1 PRA for internal events and limited Level 2 analysis or other equivalent, approved means. The various levels of PRA analysis are described in section 1.4.3. The IPE letter is the main reason PRAs are being performed by utilities today.

A summary of the insights gained from previous risk assessments are as follows:

1. As illustrated by the NUREG-1150 results (8) and previous plant PRAs, the PRAs reflect details of plant systems, operation and physical lay out. Since nuclear power plants in the U.S. are not standardized, the PRA results are very plant specific. Reactor design, equipment, location, and operation (power level, testing and maintenance, operator actions) have a large impact on the outcome. Therefore, in detail, the results can differ significantly from plant to plant.
2. Even with the differences in the detailed results between plant studies, PRA can be used for some generic applications as listed in NUREG-1050 (7). Some examples are:

   - Regulatory activity prioritization,
   - Safety issue evaluation,
   - Resource allocation,
   - Inspection program, and
   - NRC policy development.

3. Using PRA in the decision process can show which changes are desirable to improve plant safety. Example estimates of averted risk from PRA experience are listed in Table 1.4-1. This table describes plant modifications recommended by the PRA with the corresponding reduction in risk indicated as risk impact.
4. PRAs have also been used as a cost saving tool. A list of example estimates of avoided costs from PRA experience is shown in Table 1.4-2.

5. PRAs have pointed out some general differences with respect to BWRs and PWRs as a class. For example, NUREG-1150 (8) states that:

   a. Principal accident contributor to core damage frequency:
      BWRs - station blackout and ATWS
      PWRs - loss of coolant accident
   b. Core damage frequency:
      BWRs-lower than PWRs, due to more redundant systems
      PWRs -higher than BWRs, fewer ways to supply water to the reactor coolant system
   c. Early containment failure given a core damage accident:
      BWRs -higher probability
      PWRs - lower probability, due to stronger and larger containments

The major contributors to core damage by accident type for the NUREG-1150 PWR and BWR plants are shown in Figure 1.4-1.

1.4.3 Levels of PRA

A full scope PRA, calculating the risk to the public, involves three discrete levels of study. Figure 1.5-2 illustrates the activities and/or products associated with each level. The output of the three levels are as follows:

- Level 1 - plant systems modeling which computes the frequency of core damage;
- Level 2 - accident phenomenology and fission product transport analysis which computes the inventories of fission products released to the environment (source terms) and their frequencies; and
- Level 3 - consequence analysis which computes the public health effects and their likelihood from the releases of fission products.

The Level 1 PRA involves modeling plant systems and calculating frequencies of the potential accidents that could result in core damage. To identify the potential accidents and quantify their frequency of occurrence, system safety analysis methods are used (e.g., event trees, fault trees) along with initiating event frequencies, component failure data, human error rates, and common cause failure data. From this level of the PRA, the accident sequences resulting in core damage are identified and the total core damage frequency is determined.

The Level 1 PRA results provide an important quantitative measure: Core Damage Frequency. This measure is useful in efforts to manage plant safety because it is directly related to the plant systems design and operation and an indicator of the potential risk to the facility, and indirectly the public, from potential accidents. Computation of how design and operational changes effect core damage frequency indirectly indicate the impact on plant safety. Therefore, the following discussion focuses primarily on the methodology and results of the Level 1 PRA.

A set of accident sequences is the principle product of the Level 1 PRA activities. An accident sequence is a postulated occurrence consisting of an initiating event or initiating event class and a specific combination of success and failure states of the systems and/or operations which, if successful, mitigate the impact of the initiating event to maintain the plant in a safe and stable state.

Although the accident sequences of primary interest in a Level 1 lead to core damage, all these accident sequences are not equivalent. Some are more severe than others in terms of potential plant damage and/or public health consequences.

Therefore, all the Level 1 accident sequences are classified into plant damage states according to those factors which determine the potential severity of the sequences.

A Plant Damage State is a grouping of accident sequences that have the potential for similar outcomes in terms of containment response and fission product release. Characteristics of accident sequences such as reactor coolant system pressure, event timing, and system availability and operational status are considered in the development of the plant damage states. All the accident sequences with similar characteristics are put in the same plant damage state.

For example, accident sequences with containment safeguards systems failed would be put in different plant damage states from those with successful containment safeguards system operation and accident sequences with failure of emergency coolant injection put in different states than those with successful injection. Each plant damage state potentially results in a different challenge to the containment and ultimately a different inventory of fission products (source term) released to the environment.

The plant damage states define the important accident characteristics for use in the analysis of the containment response, behavior of the damaged core, and the transport of the fission products to the environment outside the containment. Therefore, the plant damage states provide the interface with the Level 2 and 3 PRA activities where the accident progression, containment response, fission product release, and subsequent risk to the public is calculated.

The output of the Level 1 PRA activities is generated principally by the use of the event tree and fault tree analysis methodology. A brief description of these methods and how they are used to determine core damage frequency is provided in the following sections.

The Level 2 PRA involves thermal hydraulic and structural analyses of containment, as well as modeling the behavior of fission products during the postulated accident. To develop and quantify these models, computer codes are utilized. From this level of the PRA, the magnitude, nature and frequency of radio nuclide releases are determined.

The Level 3 PRA involves calculating the health impact on the public from the release of the radio nuclides. To quantify the releases health effects, plume dispersion, weather characteristics (meteorology), population concentration, doses, and evacuation procedures are addressed. Computer codes are used to compute the consequences of the releases. From this level of the PRA, the number of early fatalities and delayed cancer fatalities are computed along with their likelihood.

1.4.4 Event Tree Analysis

The analytical technique used to identify accident sequences is called Event Tree Analysis. Event trees order and depict the success or failure of functions or systems required to mitigate the potential effects of an initiating event. An event tree is a simple diagram, similar to a decision tree, which merely illustrates the potential combinations of events which are of interest given some initial condition (initiating event).

To illustrate the technique, a simple event tree example has been provided. This event tree has been developed to examine the ways your instructor may fail to be here, first thing in the morning, to explain this to you.

The initiating event for this analysis is sunrise and we want to make sure that your instructor gets up and makes it to the classroom. The systems which are required to "operate" to assure that this happens are an alarm clock or wake-up call to get your instructor up, an automobile to get him or her to the building, and the elevator or the stairs to get him or her up here to the class room. The results of the event tree analysis for the instructor's failure to be in class is shown in Figure 1.4-3.

The combinations of "system" failures and successes, and the functions they perform, determine the status of the instructor (i.e., in class or absent). In event tree analysis, an upward branch (vertical line) represents a success of the system and a downward line represents a failure. Each unique combination of successes and failures is called an event tree sequence (or accident sequence). The sequences are identified by using the letters (or other identifier) corresponding to the initiating event and the systems that failed.

The sequences are developed by going through the event tree heading by heading and developing a success and failure path only in those cases where it has a bearing on the outcome (e.g., is the instructor in class or not?). Other cases which are not physically possible or do not impact the outcome are not developed. For example, when the alarm clock is successful, we do not postulate failure of the wake-up call because the instructor is already awake. Likewise, if the automobile fails, neither the elevator nor the stairs can get the instructor to class.

To demonstrate the fact that all sequences are not equal, compare sequences IAC and IAB. In IAC, the instructor is awake, but never arrives in class because either the car fails or he or she is stuck, fuming, in traffic. However, in sequence IAB, both the alarm clock and wake-up call fail to wake the instructor and he or she remains in bed sleeping (hopefully with pleasant dreams). Clearly, the effects on the instructor of these two sequences are drastically different.

For nuclear power plants, systemic event trees (event trees with systems as headings) display the combinations of plant system failures that can result in core damage. They are constructed for each initiating event group. An individual path through such an event tree (an accident sequence) identifies specific combinations of system successes and failures leading to (or avoiding) core damage. As such, the event tree qualitatively identifies what must fail in a plant in order to cause core damage.

Most initiating events for nuclear plant PRAs are those events that occur while the reactor is operating at full power, trip the plant, and require the operation of various systems to bring the reactor to a safe, stable state. Some PRAs are just starting to look at initiating events while the reactor is in other modes of operation and at events that involve the fuel storage pool. All initiating events applicable to the particular plant being analyzed must be identified along with their associated frequencies. These initiating events are collected into groups for performance of the event tree analysis.

The two kinds of initiating events considered in PRAs are:

1. Internal initiating events are those that occur mainly within the bounds of the systems being analyzed. Examples include: loss of coolant accidents, loss of offsite power, turbine trips and loss of feedwater events.
2. External initiating events are those events that generally occur outside the systems being modeled. Some examples are earthquakes, fires, and floods.

Most PRAs to date include only an analysis of internal events.

In general, a separate event tree will be developed for each initiating event group. Identification of these initiating event groups is based upon the unique combinations of mitigating systems and success criteria. For example, NUREG/CR-4550 (11) lists BWR and PWR generic transient classifications along with their associated frequencies. Specifically, two initiating event groups (or classes) for transients are identified:

1. Transients with Power Conversion System (PCS) available, and
2. Transients with loss of PCS.

This differentiation is made because if the PCS (i.e., main feedwater) is available it can be used as a heat sink, therefore, events that could result in plant trip with PCS available have different mitigating systems initially available than in the case with PCS unavailable.

The headings listed across the top of an event tree consist of those systems that mitigate the impact of the initiating event, (e.g., decay heat removal, coolant makeup systems, etc.). The required mitigating systems, referred to as front line systems in the PRA, will be identified for each initiating event. Front line systems are those systems that can perform the required safety (mitigating) functions for the initiating events or event groups. Specific success criteria, for each front line system that performs a mitigating (safety) function, must be identified. In addition to a performance definition (e.g., flow rate, response time, trip limits), these success criteria must be stated in discrete hardware terms, such as the number of required pumps, flow paths, instrument trains, or power buses. Ultimately, the success criteria for each front line system will be based on detailed thermal-hydraulic, core physics, or other phenomenological calculations.

1.4.5 Systems Analysis

The event tree analysis identifies the accident sequences that can result in core damage. Each of these sequences consists of a specific combination of an initiating event class and front line (mitigating) system failures. To identify how the systems might fail, system modeling is performed.

The most common analytical technique used to model system failures is fault tree analysis. Other modeling techniques such as expressing failure in the form of an equation or using a single failure probability number, referred to as a 'black box' model, can be used for those systems which are relatively simple and/or whose failures are independent from the other systems being analyzed. In some cases, the complexity of the system and the availability of failure data may warrant the use of data rather than a model (e.g., the main feedwater system failure is often represented by a 'black box' model).

Formally, fault tree analysis can be defined as: "an analytical technique, whereby an undesired state of the system is specified (usually a state that is critical from a safety standpoint), and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur." NUREG-0492 (12).

In other words, the fault tree is a technique to identify the ways in which a system may fail to perform its intended function. The fault tree is constructed using rules and logic symbols. It develops the ways in which a system can fail by identifying all credible single and multiple failures. The result is a logic diagram of system faults which can be evaluated by a computer.

As an example of a fault tree, let us select the alarm clock from our event tree example in Section 1.4.4. We are interested in how the alarm clock can fail to operate at sunrise. Therefore, we will develop a fault tree for the following event from the event tree: "Alarm clock fails to operate at sunrise". Figure 1.4-4 shows the start of this fault tree.

As shown in this figure, the alarm clock will fail to operate if one or more of the following fault events occur:

1. No power available to the buzzer,
2. Buzzer not commanded to buzz at sunrise, or
3. Buzzer fails.

Since the alarm clock will fail if only the buzzer fails, that fault by itself is a minimal cut set for this fault tree. While the alarm clock will also fail if both the buzzer fails and there is a loss of offsite power, this condition is more than the minimum, necessary, and sufficient set of faults and is not a minimal cut set.

If we were to complete the example fault tree, the events 'no power available to the buzzer at sunrise' and 'buzzer not commanded to buzz at sunrise' would both be developed further. The fault tree development continues until we have a tree which ends in events for which we have or can develop failure probability data and the interactions and dependencies between systems are properly addressed.

The purpose of fault tree analysis is to identify the ways in which a system can fail and provide a means to find system dependencies and subtle interactions that can contribute to multiple system failures. Fault trees are used to determine the minimal cut sets for system failure and accident sequences. The minimum, necessary, and sufficient sets of events which could result in system failure or an accident sequence are called minimal cut sets.

The fault tree includes only those fault events and logical interrelationships that contribute to the system failure identified in the event tree. Fault tree analysis is done for the front line systems and all the systems that supply required services (e.g., component cooling, AC power, or HVAC) to the front line systems. This latter type of system is referred to as a support system in the PRA. Support systems can also provide required services to other support systems (e.g., HVAC in an AC power switch gear room). Fault trees for the support systems include fault events of the systems which provide these required services.

There are generally four types of faults considered in system models. These fault events are

1. hardware failures,
2. test and maintenance errors,
3. human errors, and
4. dependent failures.

The dependent failures include faults as a result of support system failures and common cause failure of multiple components.

1.4.6 Accident Sequence Evaluation

For the Level 1 PRA, the accident sequences of interest for the evaluation process are those that are the most likely and/or potentially the most severe. The accident sequences are evaluated by computer to determine:

1. how they might occur in terms of the faults identified in the system models (qualitative results), and
2. their frequency of occurrence (quantitative results).

This evaluation is done for internal events by combining the appropriate models for the system failure events with the initiating event group for each accident sequence. Likelihood data is assigned to each event in the models, including the initiating event group. This data comes from the analysis and data bases of:

- Component failure rates,
- Maintenance frequencies,
- Human error rates,
- Common cause failure probabilities, and
- Initiating event frequencies.

For external events, the evaluation includes definition of the frequency and severity of the external event (hazard function) and the impact of the external event on the likelihood of failure of the front line and support systems.

Methodologies employed in PRAs identify the minimum set of events that could cause an accident sequence resulting in core damage. These minimum, necessary sufficient sets of events are called minimal cut sets. Minimal cut sets identify the specific system failures, and maintenance and operational errors which combine to result in an accident leading to core damage. Each type of accident sequence can occur in many different ways and thus has many different minimal cut sets.

Each minimal cut set is quantified by identifying the probability of each system fault event and the frequency of the initiating event in the cut set. All cut set frequencies for an accident sequence are combined to obtain the total sequence frequency. Those minimal cut sets that contribute approximately 90% to 95% of the total sequence frequency are called dominant cut sets. The most dominant is that cut set which contributes itself the most to the total frequency.

The frequency of all the core damage sequences are combined to calculate total core damage frequency. The set of sequences that contributes 90% to 95% of the total core damage frequency are referred to as dominant sequences. These sequences are often grouped by accident type based on the initiating event and some safety system failures.

1.4.6.1 Importance Measures

Based on the total core damage frequency and the frequency of the individual fault events, quantitative importance measures can be determined for the various accident sequences, systems, cut sets, and individual fault events. Three most often used importance measures are Percent Contribution, Risk Reduction, and Risk Achievement (or Risk Increase).

The Percent Contribution importance measure as defined for an event or system indicates the percent of the total core damage frequency which includes that event. Computing the percent contribution involves summing the frequencies of all cut sets that include the event or system of interest and dividing by the total core damage frequency. The percent contribution measure gives the percentage of the total core damage frequency associated with that event or system. Accident sequences, events or systems with a large percent contribution measure have the biggest contribution to the total core damage frequency. Because PRA includes the postulation of multiple failures, the total of the percent contribution measures often exceed 1.0. Figures 1.4-5 and 1.4-6 show the range of percent contributions for various BWR and PWR systems, respectively.

The Risk Reduction importance measure as defined for a system or event measures the sensitivity of the total core damage frequency to a decrease in the likelihood of system failure or the event of interest. First, to obtain this measure, the failure frequency of the event of interest is reduced to zero. Then, the total core damage frequency is divided by the sum of all the cut set frequencies, with the event of interest frequency at zero. Preventing or limiting that event with the largest risk reduction value will have the greatest effect in decreasing the total core damage frequency. Therefore, the risk reduction importance measure shows where the most gain can be achieved on safety improvements (e.g., the greatest decrease in total core damage frequency). Figure 1.4-7 shows the range of risk reduction for Sequoyah Safety Systems.

The Risk Achievement (or Risk Increase) importance measure as defined for a system or event measures the sensitivity of the total core damage frequency to an increase in the likelihood of the event of interest. To obtain this measure, the frequency of the event of interest is set to one. Then, the cut set frequencies are summed and divided by the total core damage frequency. The risk achievement measure identifies those areas where it is most important to verify equipment is as reliable as assumed during the initial core damage frequency calculation. The largest risk achievement measure indicates the event that should be verified reliable because it has the greatest negative impact on the total core damage frequency (e.g., the greatest increase in total core damage frequency). Figure 1.4-7 shows the range of risk achievement for Sequoyah Safety Systems.

1.4.7 Information Obtained from PRA

As mentioned in Section 1.4.3, a PRA can be performed at various levels, depending on the objectives of the study. Each discrete level, Level 1, 2, and 3, provides different information. The ultimate result of a full scope, Level 3, PRA is quantification of the risk to the public (e.g., the likelihood and number of early and latent fatalities).

The Level 1 PRA results provide an important quantitative measure: core damage frequency. Generally, the total core damage frequency for a commercial nuclear power plant is in the range of 1×10^{-4} to 1×10^{-6} per reactor year.

The qualitative results of accident sequence evaluation gives insights on the behavior of system failures leading to core damage. Minimal cut sets for the accident sequences consisting of the initiator and faults from the system models are determined. These minimal cut sets represent the sets of fault events that must exist simultaneously for the accident sequence to occur.

The Level 1 PRA accident sequence results have been used extensively to investigate generic safety issues and play a major role in rule making. Some of the more notable examples of accidents addressed by PRA include:

- Station Blackout,
- Anticipated Transients Without Scram (ATWS),
- Failure of Long Term Heat Removal (RHR Failure), and
- Inter-system (or interfacing) LOCA.

A station blackout accident sequence consists of a loss of offsite power accompanied by a total loss of onsite emergency ac power. This impacts the availability of some of the front line systems which need to operate to achieve a safe, stable shutdown. The NRC requires that every utility provide their plans for response to station blackout. PRA evaluation of station blackout accidents at nuclear power plants is described in NUREG-1032 (13).

Anticipated transients without scram (ATWS) sequences consist of a transient which would normally result in reactor trip (scram) and a failure of the systems that scram the reactor. These sequences can result in large pressure and temperature transients in the reactor coolant system and containment. PRAs have shown these types of sequences to be significant, especially at BWRs. Early discussion of the probability of failure to scram can be found in NUREG-0480 (14). Cost-benefit analysis using PRA analysis and results was done extensively during the Anticipated Transient Without Scram (ATWS) rule making process.

The failure of long term decay heat removal (residual heat removal) after a loss of coolant accident (LOCA) is another potentially significant accident sequence, especially at PWRs. A significant PRA effort was sponsored by the NRC to examine this potential accident sequence and identify potential back fits to reduce the frequency of this accident. The results of a value impact study on decay heat removal concepts are documented in NUREG/CR-2883 (15).

The Reactor Safety Study (1) identified the inter-system LOCA as a significant accident sequence for the Surry plant. This accident consists of a LOCA which violates the containment pressure boundary as a result of high pressure NSSS coolant inadvertently flowing into a low pressure line outside the containment boundary. This type of accident sequence has a very low frequency but is potentially very severe because it bypasses the containment and results in the failure of emergency core cooling.

1.4.8 Uses of PRA

The PRA Reference Document (7), NUREG-1050, addresses the many uses of PRA both on a generic and plant specific basis. However, because each nuclear power plant is essentially unique, the most powerful uses of the PRA is as a plant specific tool. PRAs can be used in two basic ways to:

1. support plant operations, maintenance, inspection, and planning activities; and
2. provide information regarding changes to improve plant safety.

The PRA supports plant activities by providing information on the risk significant areas in plant operation, maintenance and design. Then operations, maintenance, inspection, and planning can appropriately address these areas to control the risk at acceptable levels.

The risk significant areas are identified by the results of the PRA. These areas are where the most attention and effort should be focused. Several risk significant areas are: dominant contributors (indicate which failures are the largest contributors to the likelihood of accident sequences), dominant accident sequences (depict the failure paths that contribute most to core damage frequency), and importance measures (evaluate what contributes most to core damage, what would reduce the core damage frequency the most, and what has the greatest potential for increasing core damage frequency should it not be as reliable as desired).

The PRA results can be utilized in many ways during planning and operational activities of the nuclear plant. The results have an important role in risk management, training, emergency planning, maintenance planning, and risk based inspections.

1.4.8.1 Risk Management

Risk management is a means of prioritizing resources and concerns to control a level of safety. The PRA can be used during plant operation to prioritize operational and maintenance resources to maintain safety at acceptable levels. This is accomplished, in part, by periodically updating the PRA results to keep current with plant configuration and component failure. Importance measures can be used to indicate where preventive actions would be most beneficial and what is most important to maintain at acceptable safety levels. Based on the updated results, adjustments in plant activities and design can be made, as appropriate, to maintain the desired level of safety as indicated by the results of the PRA.

1.4.8.2 Operator Training and Simulator Design

Training can be emphasized for the operation of any system designated as risk significant in the PRA results. Operators can be trained on the dominant and/or most severe accident sequences identified by the PRA to improve human reliability for these situations. Assessments of instrumentation and status monitoring adequacy can be made to decrease human error rates.

1.4.8.3 Emergency Planning

Dominant accident sequences can be used to train emergency response personnel on what to expect in the event of a severe accident at a nuclear power plant. These sequences can also provide the basis for the development of guidelines for declaration of site and general emergencies. The PRA results and models can be used to aid in diagnosis and prognosis of accidents in progress.

1.4.8.4 Maintenance Planning

PRAs provide information to allow the concentration of maintenance efforts on the equipment associated with large risk achievement measures and reduce efforts in areas that have little impact on core damage. The impact on safety of potential changes to preventive and corrective maintenance practices can be measured to identify beneficial changes to improve safety.

1.4.8.5 Risk Based Inspections

The PRA provides information on dominant accident sequences and their minimal cut sets. Some PRAs have already been used to design the risk based portion of plant inspection programs (16), NUREG/CR-5058. Inspection programs can be prioritized to address the minimization of hardware challenges, the assurance of hardware availability, and the effectiveness of plant staff actions as they relate to the systems and faults included in the dominant accident sequences.

PRA supports the assessment of plant changes by providing quantitative measures of the relative level of safety of each change. This is accomplished by performing sensitivity studies. A sensitivity study is a study of how different assumptions, configurations, data or other potential changes in the basis of the PRA impact the results.

1.4.8.6 Design Trade Studies

To analyze the impact of various proposed designs with respect to their quantitative impact on risk, the PRA is reevaluated for each different design. This provides a relative measure of the potential positive (or negative) impact each design will have with respect to plant risk due to severe accidents.

1.4.8.7 Backfit Decisions

There are many cases where PRAs have been used to support the back fit decision process. After the TMI accident several TMI action plan issues evolved. Consumers Power performed a PRA of the Big Rock Point nuclear power plant to assist in identifying those TMI generated changes which might actually have an impact on the risk at the plant. As a result, Consumers Power was able to negotiate exemptions on seven of the issues that did not significantly lower risk at Big Rock Point, saving over $45 million (7). In addition, Consumers Power used the PRA to identify changes necessary to reduce the core damage frequency at Big Rock Point to acceptable levels.

1.4.8.8 Procedural Changes

Changes to procedures are often recommended as a result of the PRA. For example, a PRA done on Arkansas Nuclear One identified several procedural changes to reduce the probability of core damage (7). One included staggering the quarterly tests on the station batteries to reduce the probability of common cause failures in the dc power supply.

1.4.8.9 Cost-benefit Analysis

By considering the cost of the changes analyzed by the PRA, a cost-benefit analysis can be accomplished. The cost of a change is generally considered to be the cost associated with it in dollars, including the cost of design, licensing, implementation, operation and maintenance. Sometimes the cost of replacement power is included for back fits requiring plant shut down to implement. The benefit of the change is the reduction in risk if the change is implemented. The most cost effective change of all those that achieve acceptable safety, is the one which provides the most improvement in safety for the least cost. This type of cost-benefit analysis was done extensively during the Anticipated Transient Without Scram (ATWS) rule making process.

1.4.9 Inspection Effort

It is increasingly important to be familiar with PRA activities and results mainly because of the increased use of the results in plant operation and licensing. As mentioned, the NRC issued a letter to initiate an Individual Plant Examination (IPE) Program for Severe Accident Vulnerabilities (9). The NRC is requesting each licensed nuclear power plant to identify plant specific vulnerabilities to severe accidents by performance of a Level 1 PRA for internal events and limited Level 2 analysis or other equivalent, approved means.

As a plant inspector, you will be expected to use PRA results to assist in prioritizing your activities at the plant. NRC has used PRA information to support the activities of the operational assessment and readiness (OAR) team reviews of safety significant equipment and actions.

You will need to be alert for situations in the plant which constitute near misses. That is, you need to recognize those events that bring the plant close to an accident sequence occurrence. For example, the service water system (SWS) at a BWR was contaminated with silt. This increased the probability of common cause failure of the redundant valves in the SWS. Because the SWS is a support system for many other systems, this resulted in a significant increase in the likelihood of core damage at the plant. Recognizing the significance of events at the plant is especially true for those related to sequences such as ATWS and inter-system LOCA which can have severe consequences.

Finally, you will find yourself in more and more discussions where PRA results are being used or misused to justify a particular action or inaction. Therefore, it is important that you are familiar with the types of information a PRA provides and can use the PRA information accurately in your discussions and decisions.

1.4.10 Summary

PRA has become a part of the safety culture of both the NRC and the utilities. The IPE letter requires that every operating plant have a Level 1 PRA or equivalent.

The Level 1 PRA uses event trees to identify potential accident sequences that could result in core damage and fault trees to identify the system faults that can result in accident sequences. The event trees and the fault trees are used to determine:

1. How accident sequences might occur in terms of the faults identified in the system models (qualitative results), and
2. The frequency of occurrence (quantitative results).

By computing quantitative measures of risk, PRA provides the means to identify the relative importance of accident sequences, systems, and events to plant safety. Because of this characteristic of the PRA results, it is being widely used to assist in plant operations and planning, and to assess the impact of potential design and operational changes on plant safety.

Currently, the PRA methods and results are being used to assist the NRC in addressing potential nuclear power plant accident sequences of concern. Among these are station blackout, ATWS, failure of long term decay heat removal, and the inter-system (interfacing) LOCA.

1.4.11 References

1. "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", (WASH-1400) NUREG-75/014, U.S. Nuclear Regulatory Commission, Washington, DC, October 1975.

2. "Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission", NUREG/CR-0400, September 1978.

3. "Report of the President's Commission on the Accident at Three Mile Island", J.G. Kemeny et al., October 1979.

4. "Three Mile Island - A Report to the Commissioners and to the Public", NUREG/CR-1250, Vol. 1, January 1980.

5. "Interim Reliability Evaluation Program Procedures Guide", NUREG/CR- 2728, U.S. Nuclear Regulatory Commission, Washington, DC, January 1983.

6. "PRA Procedures Guide", NUREG/CR-2300, U.S. Nuclear Regulatory Commission, Washington, DC, January 1983.

7. "Probabilistic Risk Assessment Reference Document", NUREG-1050, U.S. Nuclear Regulatory Commission, Washington, DC, September 1984.

8. "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants", NUREG-1150, U.S. Nuclear Regulatory Commission, June 1989.

9. "Individual Plant Examination for Severe Accident Vulnerabilities", Generic Letter No. 88-20, U.S. Nuclear Regulatory Commission, Washington, DC, November 1988.

10. "Fundamentals of PRA", Idaho National Engineering Laboratory, Idaho Falls, ID, January 1990.

11. "Analysis of Core Damage Frequency: Internal Events Methodology", NUREG/CR-4550, Vol. 1, Rev. 1, SAND86-2048, Sandia National Laboratories, Albuquerque, NM, January 1990.

12. "Fault Tree Handbook", NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, DC, January 1981.

13. "Evaluation of Station Blackout Accidents at Nuclear Power Plants - Technical Findings Related to Unresolved Safety Issue A-44", NUREG-1032, U.S. Nuclear Regulatory Commission, Washington, DC, June 1988.

14. "Anticipated Transients Without Scram for Light Water Reactors", NUREG- 0480, Vol. 1, U.S. Nuclear Regulatory Commission, Washington, DC, April 1978.

15. "Study of the Value and Impact of Alternative Decay Heat Removal Concepts for Light Water Reactors", NUREG/CR-2883, Vol. 1,2,3, U.S. Nuclear Regulatory Commission, Washington, DC, June 1985.

16. "PRA Applications Program for Inspection at ANO-1", NUREG/CR-5058, U.S. Nuclear Regulatory Commission, Washington, DC, March 1988.

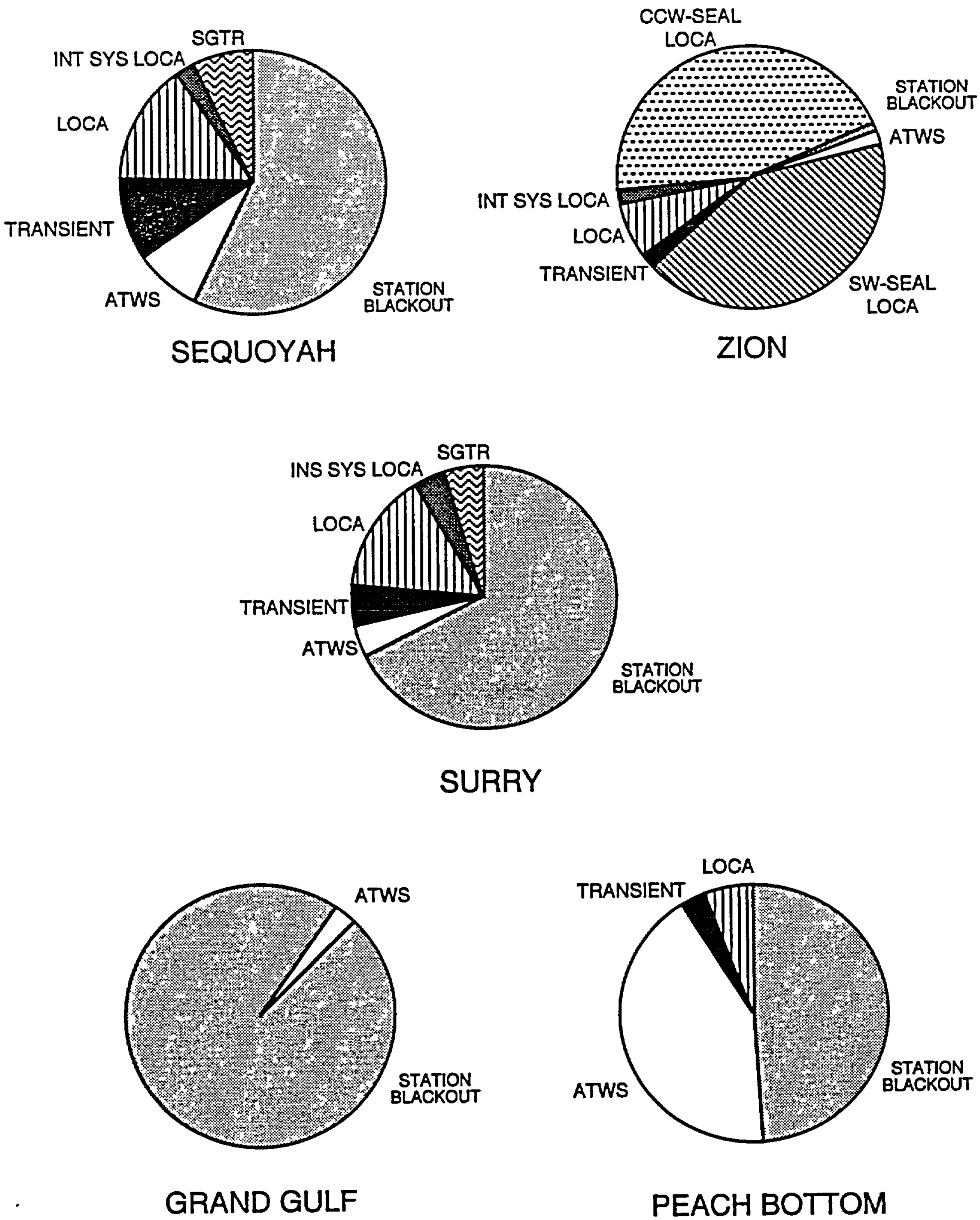
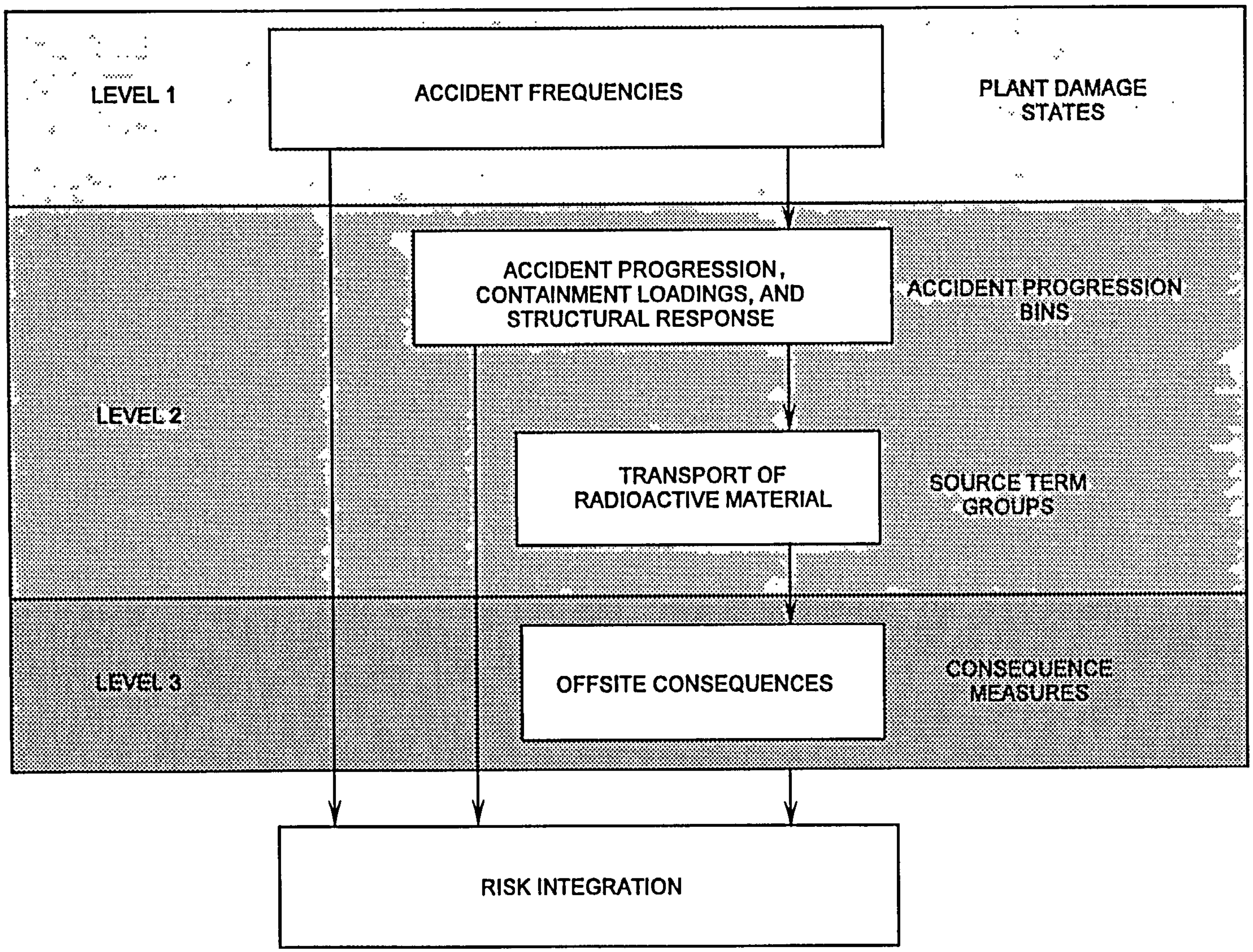


Figure 1.4-1 Major Contributors To Core Damage By Accident Types



NOTE: ADAPTED FROM NUREG-1150

Figure 1.4-2 Principal Steps in Risk Anlaysis Process

0199-3

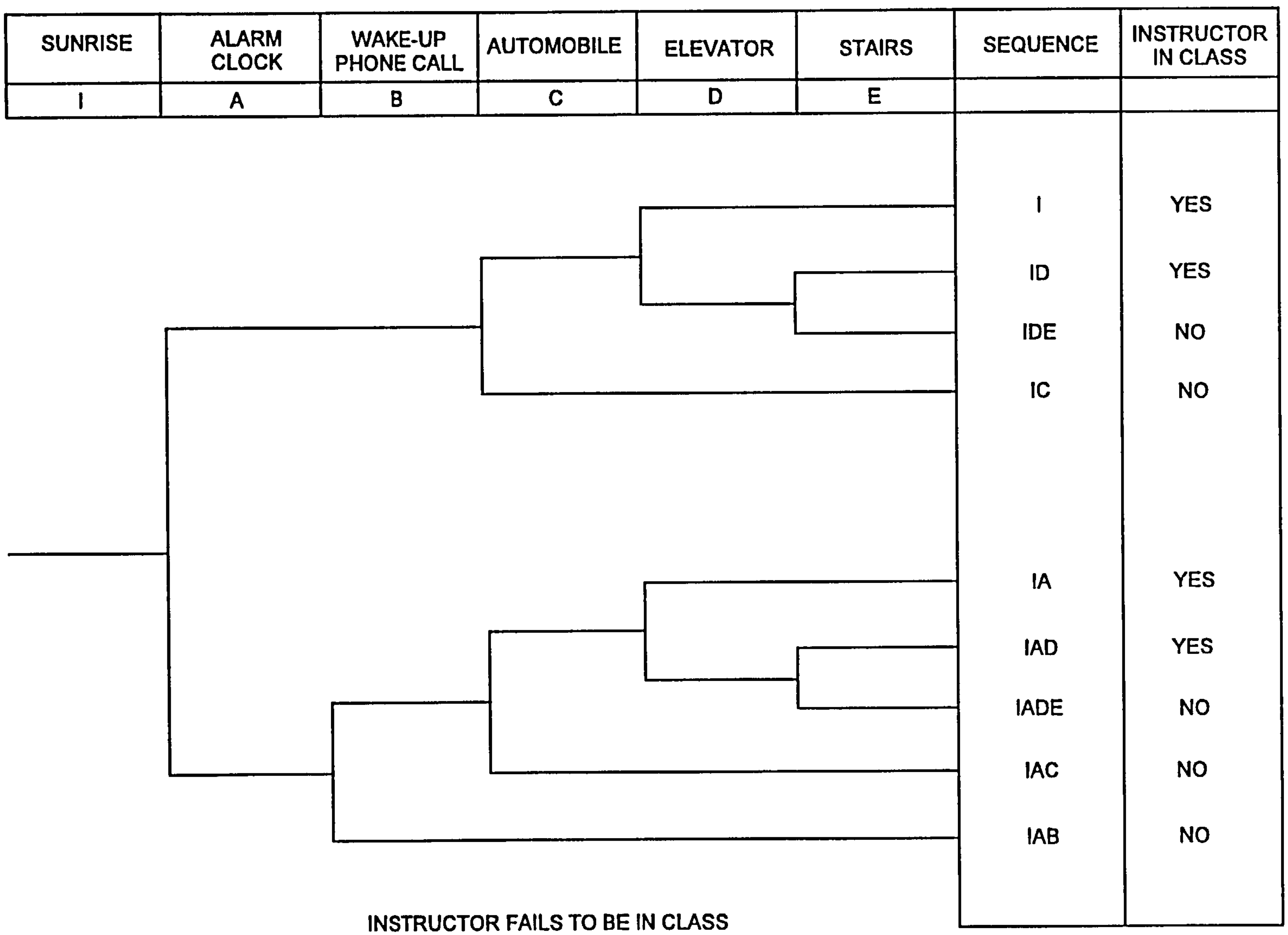
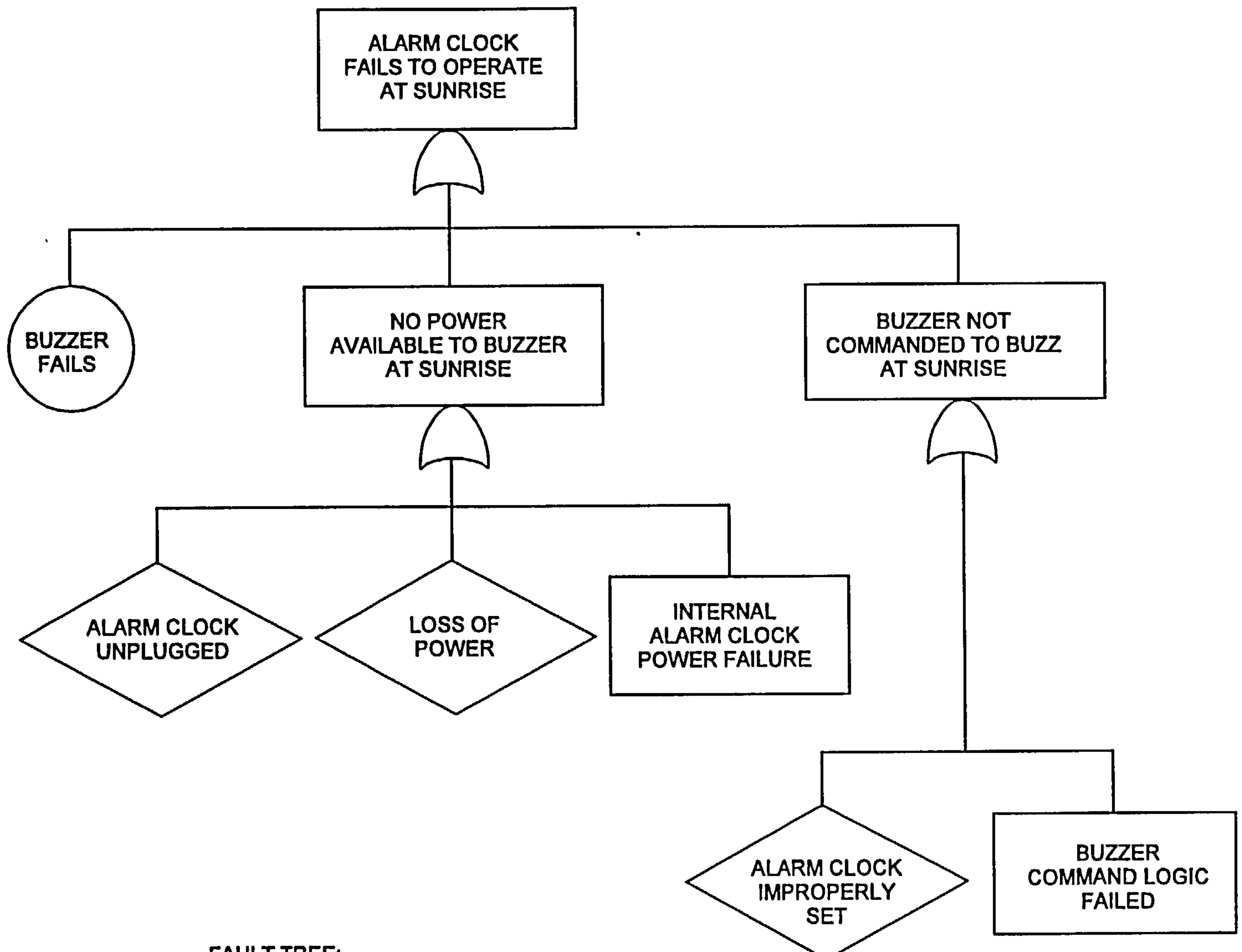


Figure 1.4-3 Event Tree Analysis

0199-3



FAULT TREE:
ALARM CLOCK FAILS TO OPERATE

Figure 1.4-4 Fault Tree

0199-3

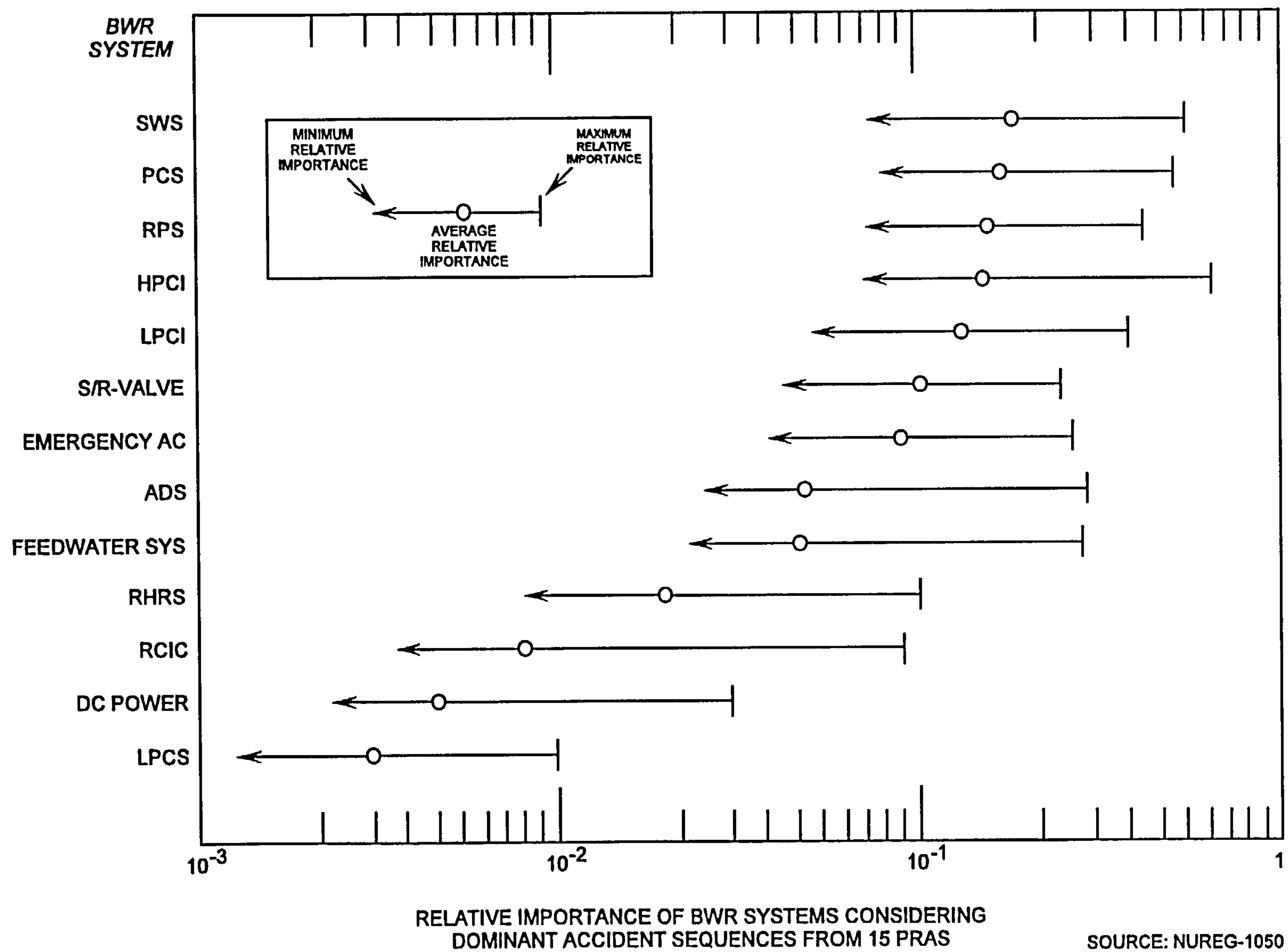


Figure 1.4-5 Relative Importance Factors

0199-3

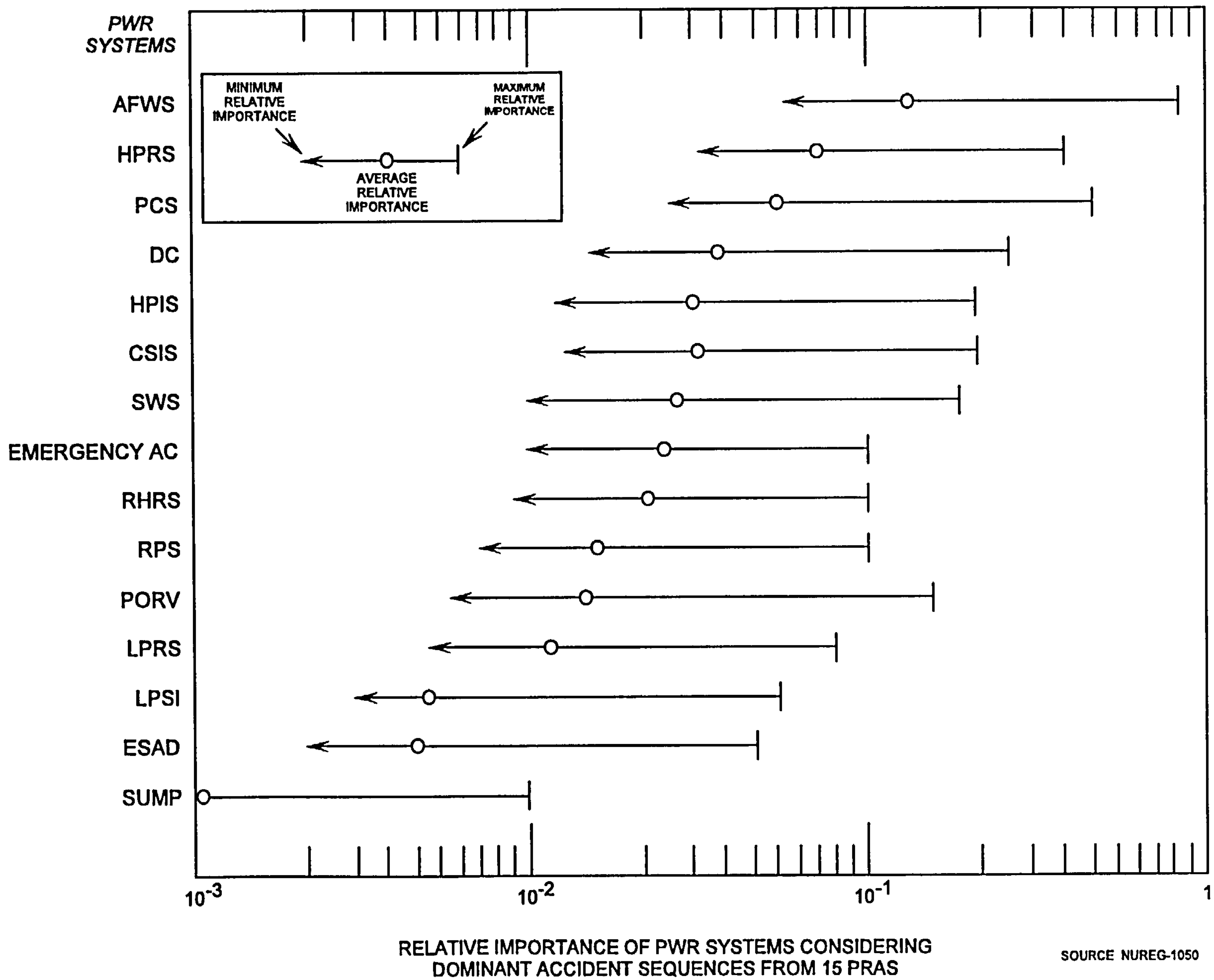
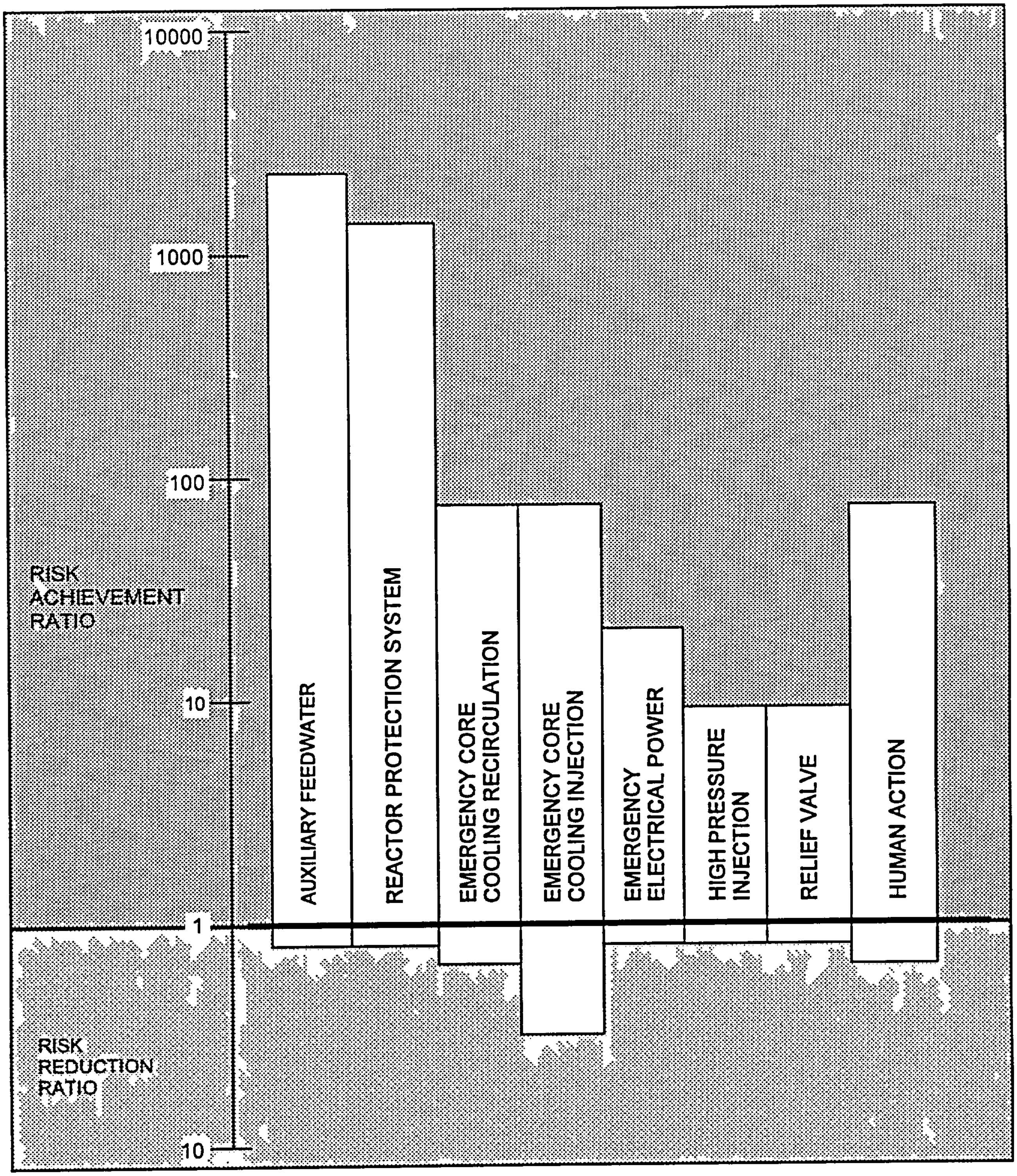


Figure 1.4-6 Relative Importance Factors

0199-3



NOTE: RISK-WORTH RATIOS FOR SEQUOYAH SAFETY SYSTEMS WITH REGARD TO CORE-MELT FREQUENCY.
SOURCE: NUREG-1050

Figure 1.4-7 Risk-Worth Ratios