CHAPTER 7

CONTENTS

CONTENTS (cont)

CONTENTS (cont)

CONTENTS (cont)

CONTENTS (cont)

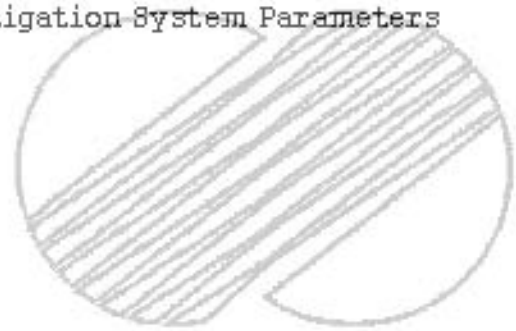
216

Amendment 216
2003. 6. 17

CONTENTS (cont)

TABLES

TABLES (cont)



FIGURES

FIGURES (cont)

216

7. INSTRUMENTATION AND CONTROLS

7.1 INTRODUCTION

This chapter presents the various plant instrumentation and control systems by relating the functional performance requirements, design bases, system descriptions, design evaluations, and tests and inspections for each. The information provided in this chapter emphasizes those instruments and associated equipment which constitute the protection system as defined in IEEE Standard 279, Criteria for Protection Systems for Nuclear Power Generating Stations.

The primary purpose of the instrumentation and control systems is to provide automatic protection and to exercise proper control against unsafe and improper reactor operation during steady-state and transient power operations (American Nuclear Society (ANS) Conditions I, II, III) and to provide initiating signals to mitigate the consequences of faulted conditions (ANS Condition IV). ANS conditions are discussed in chapter 15. Consequently, the information presented in this chapter emphasizes those instrumentation and control systems which are central to assuring that the reactor can be operated to produce power in a manner that ensures no undue risk to the health and safety of the public.

It is shown that the applicable criteria and codes, such as the USNRC General Design Criteria and IEEE Standards, concerned with the safe generation of nuclear power, are met by these systems.

A. Definitions

Terminology used in this chapter is based on the definitions given in IEEE Standard 279 which is listed in subsection 7.1.2. In addition, the following definitions apply:

1. Degree of Redundancy - The difference between the number of channels monitoring a variable and the number of channels which, when tripped, will cause an automatic system trip.

2. Minimum Degree of Redundancy - The degree of redundancy below which operation is prohibited or otherwise restricted by the technical specifications.

3. Cold Shutdown Condition – When the reactor is subcritical by at least 1 percent $\Delta k/k$ and T_{avg} is $\leq 200^{\circ}F$.

4. Hot Shutdown Condition – When the reactor is subcritical by an amount greater than or equal to the margin to be specified in the applicable technical specification and T_{avg} is greater than or equal to the temperature specified in the applicable technical specification.

5. Phase A Containment Isolation – Closure of all nonessential process lines which penetrate containment initiated by the safety injection signal.

6. Phase B Containment Isolation – Closure of remaining process lines, initiated by containment Hi-3 pressure signal (process lines do not include engineered safety features (ESF) lines).

B. System Response Times

1. Reactor Trip System Response Time – The reactor trip system response time shall be the time interval from when the monitored parameter exceeds its trip setpoint at the channel sensor until loss of voltage to the stationary gripper coils.

2. Engineered Safety Features Actuation System Response Time – The interval required for the ESF sequence to be initiated subsequent to the point in time that the appropriate variable(s) exceed set points. The response time includes sensor/process (analog) and logic (digital) delay plus the time delay associated with tripping open the reactor trip breakers and control and latching mechanisms, although the ESF actuation signal occurs before or simultaneously with ESF sequence initiation (see figure 7.2-1, sheet 8).

C. Reproducibility

This definition is taken from Scientific Apparatus Manufacturers Association (SAMA) Standard PMC-20.2-1973, Process Measurement and Control Terminology: "the closeness of agreement among repeated measurements of the output for the same value of input, under normal operating conditions over a period of time, approaching from both directions." It includes drift due to environmental effects, hysteresis, long-term drift, and repeatability. Long-term drift (aging of components, etc.) is not an important factor in accuracy requirements since, in general, the drift is not significant with respect to the time elapsed between testing. Therefore, long-term drift may be eliminated from this definition. Reproducibility, in most cases, is a part of the definition of accuracy (see below).

D. Accuracy

This definition is derived from Scientific Apparatus Manufacturers Association (SAMA) Standard PMC-20.1-1973, Process Measurement and Control Terminology. An accuracy statement for a device falls under Note 2 of the SAMA definition of accuracy, which means reference accuracy or the accuracy of that device at reference operating conditions: "Reference accuracy includes conformity, hysteresis, and repeatability." To adequately define the accuracy of a system, the term reproducibility is useful as it covers normal operating conditions. The following terms, "trip accuracy" and "indicated accuracy" etc., will then include conformity and reproducibility under normal operating conditions. Where the final result does not have to conform to an actual process variable but is related to another value established by testing, conformity may be eliminated, and the term reproducibility may be substituted for accuracy.

E. Normal Operating Conditions

These conditions cover all normal process temperature and pressure changes. Also included are ambient temperature changes around the transmitters and racks. Accuracies under post-accident conditions are not included.

F. Readout Devices

For consistency, the final device of a complete channel is considered a readout device. This includes indicators, recorders, isolators (non-adjustable) and controllers.

G. Channel Accuracy

This definition includes accuracy of primary element, transmitter, and rack modules. It does not include readout devices or rack environmental effects, but does include process and environmental effects on field-mounted hardware. Rack environmental effects are included in the next two definitions to avoid duplication due to dual inputs.

H. Indicated and/or Recorded Accuracy

This definition includes channel accuracy, accuracy of readout devices, and rack environmental effects.

I. Trip Accuracy

This definition includes comparator accuracy, channel accuracy for each input, and rack environmental effects. This is the tolerance expressed in process terms (or percent of span) within which the complete channel must perform its intended trip function. This includes all instrument errors but no process effects, such as streaming. The term "actuation accuracy" may be used where the word "trip" might cause confusion (for example, when starting pumps and other equipment).

J. Control Accuracy

This definition includes channel accuracy, accuracy of readout devices (isolator, controller), and rack environmental effects. Where an isolator separates control and protection signals, the isolator accuracy is added to the channel accuracy to determine control accuracy, but credit is taken for tuning beyond this point: i.e., the accuracy of these modules (excluding controllers) is included in the original channel accuracy. It is simply defined as the accuracy of the control signal in percent of the span of that signal. This will then include gain changes where the control span is different from the span of the measured variable. Where controllers are involved, the control span is the input span of the controller. No error is included for the time in which the system is in a non-steady-state condition.

7.1.1 IDENTIFICATION OF SAFETY-RELATED SYSTEMS

7.1.1.1 Safety-Related Systems

The instrumentation that is required to function to achieve the system responses assumed in the safety evaluations, and those needed to shut down the plant safely, are given in this subsection.

Table 7.1-1 provides a tabulation of design responsibility and reference plant for plant instrumentation systems.

7.1.1.1.1 Reactor Trip System

The reactor trip system (RTS) is a functionally defined system described in section 7.2. The equipment which provides the trip functions is identified and discussed in section 7.2. Design bases for the reactor trip system are given in subparagraph 7.1.2.1.1. This system is shown in figure 7.1-1.

7.1.1.1.2 Engineered Safety Features Actuation System

The engineered safety features actuation system (ESFAS) is a functionally defined system described in section 7.3. The equipment which provides the actuation functions is identified and discussed in section 7.3. Design bases for the ESFAS are given in subparagraph 7.1.2.1.2.

7.1.1.1.3 Instrumentation and Control Power Supply System

Design bases for the instrumentation and control power supply system are given in subparagraph 7.1.2.1.3. Further description of this system is provided in subsection 7.6.1.

7.1.1.1.4 Systems Required for Safe Shutdown

Systems required for safe shutdown are defined as those essential for pressure and reactivity control, coolant inventory makeup, and removal of residual heat once the reactor has been brought to a subcritical condition.

Identification of the equipment and systems required for safe shutdown is provided in section 7.4. Additional information regarding hot standby provisions for shutdown from outside the control room is also provided in section 7.4.

7.1.1.1.5 Safety-Related Display Instrumentation

Display instrumentation provides the operator with information to monitor the results of ESF action following a Condition II, III or IV event. Section 7.5, table 7.5-1, identifies the safety-related display information.

7.1.1.1.6 All Other Instrumentation Systems Required for Safety

The other instrumentation systems required for safety (other than the RTS, the ESFAS, safety-related display, and the safe shutdown systems) are discussed in section 7.6. They are those systems and components that have a preventive role in reducing the effects of accidents. Single failures in these systems will not inhibit reactor trip, ESF actuation, or functions required for safe shutdown. The other instrumentation systems required for safety consist of the following:

A. Instrumentation and control power supply system
B. Residual heat removal isolation valve interlocks
C. Refueling interlocks
D. Accumulator motor-operated valve interlocks
E. Emergency core cooling system (ECCS) switchover from injection mode to recirculation mode
F. Interlocks for RCS pressure control during low temperature operation
G. Isolation of non-Seismic Category I Piping from Seismic Category I cooling system.

Design bases for instrumentation and control power supply system are given in paragraph 7.1.2.1. Further description of this system is provided in subsection 7.6.1 and section 8.3. Item C is described in subsection 9.1.4, and the remaining items are described in section 7.6.

7.1.1.2 Instrumentation and Control System Designers

All systems discussed in chapter 7 have definitive functional requirements developed on the basis of the Westinghouse NSSS design. All equipment necessary to achieve the functions shown on the logic diagrams, figure 7.2-1, are supplied by the NSSS except where noted on the diagrams as being BOP supplied.

7.1.1.3 Plant Comparison

System functions for all systems discussed in chapter 7 are similar to those of the KORI Nuclear Units 3 & 4 (KRN 3 & 4) application. A comparison table is provided in section 1.3.

7.1.2 IDENTIFICATION OF SAFETY CRITERIA

Paragraph 7.1.2.1 gives design bases for the systems listed in paragraph 7.1.1.1. Design bases for nonsafety-related systems and other safety-related systems are provided in the sections which describe the systems. Conservative considerations for instrument errors are included in the accident analyses presented in chapter 15. Functional requirements, developed on the basis of the results of the accident analyses, which utilize conservative assumptions and parameters, are used in designing these systems, and a preoperational testing program verifies the adequacy of the design. Accuracies are given in sections 7.2, 7.3, and 7.5.

The documents listed in table 7.1-2 were considered in the design of the systems given in paragraph 7.1.1.1. In general, the scope of each document is given in the document itself. This determines the system or parts of systems to which the document is applicable. A discussion of compliance with each document for systems within its scope is provided in the referenced sections. Because some documents were issued after design and testing had been completed, the equipment document may not meet the format requirements of some standards. Justification for any exceptions taken to each document for systems in its scope is provided in the referenced sections.

7.1.2.1 Design Bases

7.1.2.1.1 Reactor Trip Systems

The reactor trip system acts to limit the consequences of Condition II events (faults of moderate frequency), such as loss of feedwater flow by, at most, a shutdown of the reactor and turbine, with the plant capable of returning to operation after corrective action. The reactor trip system features impose a limiting boundary region to plant operation which ensures that the reactor safety limits are not exceeded during Condition II events and that these events can be accommodated without developing into more severe conditions. Reactor trip setpoints are given in ITS Chapter 1. | 348

The design requirements for the reactor trip system are derived by analyses of plant operating and fault conditions where automatic rapid control rod insertion is necessary in order to

prevent or limit core or reactor coolant pressure boundary damage. The design bases addressed in Section 3 of IEEE Standard 279 are discussed in subsection 7.2.1. The design limits specified for the reactor trip system are:

A. Minimum departure from nucleate boiling ratio (DNBR) shall not be less than 1.30 as a result of any anticipated transient or malfunction (Condition II faults).

B. Power density shall not exceed the rated linear power density for Condition II faults. See chapter 4 for fuel design limits.

C. The stress limit of the reactor coolant system (RCS) for the various conditions shall not be exceeded as specified in chapter 5.

D. Release of radioactive material shall not be sufficient to interrupt or restrict public use of those areas beyond the exclusion radius as a result of any Condition III fault.

E. For any Condition IV fault, release of radioactive material shall not result in an undue risk to public health and safety.

7.1.2.1.2 Engineered Safety Features Actuation System

The engineered safety features actuation system (ESFAS) acts to limit the consequences of Condition III events (infrequent faults such as primary coolant leakage from a small rupture which exceeds normal charging system makeup and requires actuation of the safety injection system). The ESFAS acts to mitigate Condition IV events (limiting faults, which include the potential for significant release of radioactive material).

The design bases for the ESFAS are derived from the design bases given in chapter 6 for the ESF. Design bases requirements of Section 3 of IEEE Standard 279 are addressed in paragraph 7.3.1.2. General design requirements are given below:

A. Automatic Actuation Requirements

The primary requirement of the ESFAS is to receive input signals from the various processes within the reactor plant and containment, and automatically

provide, as output, timely and effective signals to actuate the various components and subsystems comprising the ESF system.

B. Manual Actuation Requirements

The ESFAS has provisions in the control room for manually initiating the functions of the ESF system.

7.1.2.1.3 Instrumentation and Control Power Supply System

The instrumentation and control power supply system provides continuous, reliable, regulated single-phase ac power to all instrumentation and control equipment required for plant safety. Details of this system are provided in section 7.6 and chapter 8. The design bases are given below:

A. Each inverter or regulating transformer has the capacity and regulation required for the ac output for proper operation of the equipment supplied.

B. Redundant loads are assigned to different distribution panels which are supplied from different inverters or regulating transformers.

C. Auxiliary devices that are required to operate dependent equipment are supplied from the same distribution panel to prevent the loss of electric power in one protection set from causing the loss of equipment in another protection set. No single failure shall cause a loss of power supply to more than one distribution panel.

D. Each of the distribution panels has access only to its respective inverter or regulating transformer supply and a standby regulating transformer power supply.

E. The system complies with IEEE Standard 308, Paragraph 5.4.

7.1.2.1.4 Emergency Power

Design bases and system description for the emergency power supply are provided in chapter 8.

7.1.2.1.5 Interlocks

Interlocks are discussed in sections 7.2, 7.3, 7.6, and 7.7. The protection (P) interlocks for the reactor trip system and the ESFAS are given in tables 7.2-2 and 7.3-2, respectively. The safety analyses demonstrate that even under conservative critical conditions for either postulated or hypothetical accidents, the protective systems ensure that the NSSS will be put into and maintained in a safe state following an ANS Condition II, III, or IV accident commensurate with applicable technical specifications and pertinent ANS criteria. Therefore, the protective systems have been designed to meet IEEE Standard 279 and are entirely redundant and separate, including all permissives and blocks. All blocks of a protective function are automatically cleared whenever the protective function would be required to operate in accordance with General Design Criteria 20, 21, and 22 and Paragraphs 4.11, 4.12, and 4.13 of IEEE Standard 279. Control interlocks (C) are identified in table 7.7-1. Because control interlocks are not safety-related, they have not been specifically designed to meet the requirements of IEEE Protection System Standards.

7.1.2.1.6 Bypasses

Bypasses are designed to meet the requirements of IEEE Standard 279 Sections 4.11, 4.12, 4.13, and 4.14. A discussion of bypasses provided is given in sections 7.2 and 7.3.

7.1.2.1.7 Equipment Protection

The criteria for equipment protection are given in chapter 3. Equipment related to safe operation of the plant is designed, constructed, and installed to protect it from damage. This is accomplished by working to accepted standards and criteria aimed at providing reliable instrumentation which is available under varying conditions. In general, all BOP safety-related equipment and certain NSSS-supplied equipment are seismically qualified in accordance with IEEE Standard 344. During construction, independence and separation is achieved, as required by IEEE Standard 279, IEEE Standard 384 and Regulatory Guide 1.75 either by barriers or physical separation or by analysis or test. This serves to protect against complete destruction of a system by fires, missiles or other natural hazards. A discussion of the overcurrent relaying as applied to Class 1E electrical equipment is given in subparagraph 8.3.1.1.2.11.

7.1.2.1.8 Diversity

Functional diversity has been designed into the ESFAS and the reactor trip system. Functional diversity is discussed in reference 1. The extent of diverse system variables has been evaluated for a wide variety of postulated accidents as discussed in reference 2. Generally, two or more diverse protection functions would automatically terminate an accident before unacceptable consequences could occur.

For example, there are automatic reactor trips based upon neutron flux measurements, reactor coolant loop temperature measurements, pressurizer pressure and level measurements, reactor coolant pump underfrequency, and undervoltage measurements, as well as manually, and by initiation of a safety injection signal.

Regarding the ESFAS for a loss-of-coolant accident, a safety injection signal can be obtained manually or by automatic initiation from three diverse parameter measurements.

A. Low pressurizer pressure

B. High containment pressure (Hi-1)

C. Low steam line pressure.

For a steam line break accident, diversity of safety injection signal actuation is provided by:

A. Low compensated steam line pressure

B. Low pressurizer pressure

C. For a steam break inside containment, high containment pressure (Hi-1) provides an additional parameter for generation of the signal.

All of the above sets of signals are redundant and physically separated and meet the requirements of IEEE Standard 279.

7.1.2.1.9 Trip Set Points

The guidelines of Regulatory Guide 1.105, Rev. 1 (11/76), are followed with the clarification described below.

The protection system will automatically initiate appropriate protective action whenever a condition monitored by the system reaches a preset condition or set point.

Three groups of values are used in determining reactor trip and ESF actuation set points.

The first group of values will be the safety analysis limits assumed in the accident analyses (chapter 15). These will be the least conservative values.

The second group will consist of limiting values as listed in
848 ITS Chapter 1. These will be the maximum/minimum "Allowable Values" for limiting safety system settings (LSSS) and limiting conditions for operation (LCO). Limiting values will be obtained by subtracting a safety margin from the accident analysis values. The safety margin will account for instrument error, calibration uncertainties, and process uncertainties such as flow stratification and transport factor effects, etc.

The third group will consist of the nominal values set into the equipment. These values will be obtained by subtracting allowances for instrument drift from the limiting values. The nominal values will allow for normal expected instrument set point drift such that the technical specification "Allowable Values" will not be exceeded under normal operation. These
848 values are given as the "Trip Set Points" in ITS Chapter 1.

As illustrated above, the trip set point will be determined by factors other than the most accurate portion of the instrument's range. The only requirement on the instrument's accuracy value is that over the instrument span, the error must always be less than equal to that assumed in the accident analyses. The instrument does not need to be the most accurate at the trip set point value as long as it meets the minimum accuracy requirements.

Range selection for the instrumentation will cover the expected range of the process variable being monitored consistent with its application. The design of the protection system is such that trip set points do not require process transmitters to operate within 5 percent of the high and low end of their calibrated span or range. Functional requirements established for every channel in the protection system stipulate the maximum allowable errors on accuracy, linearity, and reproducibility. The protection channels have the capability to ensure and to be tested to ascertain that the characteristics throughout the entire span are acceptable and meet functional requirements specifications.

In this regard it should be noted that specific functional requirements for response time, set point, and operating span will be finalized contingent on the results and evaluation of safety studies to be carried out using data pertinent to Korea Nuclear Units 7 and 8. Emphasis will be placed on establishing adequate performance requirements under both normal and faulted conditions. This will include consideration of process transmitter margins such that even under a highly improbable situation of full power operation at the safety limits that adequate instrumentation response is available to ensure plant safety.

7.1.2.1.10 Engineered Safety Features Motor Specifications

Engineered safety features motor specifications are discussed in chapter 8.

7.1.2.2 Independence of Redundant Safety-Related Systems

The safety-related systems listed in paragraph 7.1.1.1 are designed to meet the independence and separation requirements of Criterion 22, of 10 CFR 50, Appendix A, General Design Criteria, and Paragraph 4.6 of IEEE Standard 279.

The electrical power supply, instrumentation, and control conductors for redundant circuits have physical separation to preserve the redundancy and to ensure that no single credible event will prevent operation of the associated function due to electrical conductor damage. Critical circuits and functions include power, control, and analog instrumentation associated with the operation of the reactor trip system or ESFAS. Credible events include, but are not limited to, the effects of short circuits, pipe rupture, missiles, fire, etc., and are considered in the basic plant design.

7.1.2.2.1 General (Including IEEE 384 and Regulatory Guide 1.75)

Description of the field wiring for redundant circuitry is provided in section 8.3.

The physical separation criteria for redundant safety-related system sensors, sensing lines, wireways, cables, and components on control boards/racks for the NSSS meet recommendations contained in IEEE 384 and Regulatory Guide 1.75, with the following comments:

A. Separation recommendations for redundant instrumentation racks are not the same as those given in Paragraph C16 of Regulatory Guide 1.75, Revision 2.

for the control boards containing redundant circuits which are required to be physically separated from each other. However, since there are no redundant circuits that share a single compartment of an NSSS protection instrumentation rack, and since these redundant protection instrumentation racks are physically separated from each other, the physical separation requirements specified for the main control board do not apply.

However, since isolator verification tests did not include cabinet wiring, the NRC Staff expressed concerns about the operation of the devices as installed in the cabinets. The concern was that the electrical wiring, to (input) and from (output) the isolators, because of heir close proximity to each other in the as-built equipment, might permit control-side faults to enter the protection system through input-output electrical coupling and in effect bypassing the isolator.

To demonstrate the adequacy of the designs, Westinghouse conducted test programs to supplement the isolator verification tests in order to assess any effects due to the manner in which isolators were wired in the protection cabinets.

Westinghouse test programs have demonstrated that Class 1E protection systems, nuclear instrumentation system (NIS), solid-state protection system (SSPS), and 7300 process control system (7300 PCS), are not degraded by non-Class 1E circuits sharing the same enclosure. Conformance to the requirements of IEEE-279 and Regulatory Guide 1.75 has been established and accepted by the NRC.

Tests conducted on the as-built designs of the NIS and SSPS were reported and accepted by the NRC in support of the Diablo Canyon application (Docket Nos. 50-275 and 50-323). Westinghouse considers these programs as applicable to all plants, including YGN 1 & 2. Westinghouse tests on the 7300 PCS were covered in a eport entitled "7300 Series Process Control System Noise Tests", subsequently reissued as WCAP-8892 (reference 3). In a letter dated April 20, 1977, R. Tedesco to C. Eicheldinger, the NRC accepted the report.

B. The physical separation criteria for instrument cabinets within Westinghouse NSSS scope meet the recommendations contained in Paragraph 5.7 of IEEE-384.

For balance of plant equipment, conformance to the recommendations and requirements contained in IEEE 384 and Regulatory Guide 1.75, is discussed below.

Isolation devices are used to ensure that failures in nonsafety-related equipment do not prevent safety-related equipment from performing their assigned actions. Switches, relays, optical and electronic couplers are used for digital signals. Amplifiers, transducers, current transformers and fuses are used for analog signals.

Isolation devices are designed to meet the criteria for design of Class 1E equipment specified in subsection 7.1.2 and subparagraph 8.1.5.2.2. The isolation function shall not be impaired by overcurrents, short circuits, abnormal voltages, abnormal ambient, nor other credible events as specified for individual applications. All isolation devices are qualified by tests and/or analysis. The qualification of isolation devices are based on criteria specified in subsection 7.1.2 and subparagraph 8.1.5.2.2. The separation in connection with isolation devices is discussed in paragraph 8.3.1.4.

7.1.2.2.2 Specific Electrical Separation Criteria

The electrical conductors for power supply, instrumentation, and control circuits have physical and electrical separation to preserve redundancy and to ensure that no single credible event will prevent operation of the required safety system functions. Credible events include, but are not limited to, the effects of fire, short circuits, pipe rupture, missiles, etc. Electrical separation required for protection against plant events are included in the basic plant design in accordance with IEEE-384 and Regulatory Guide 1.75.

Channel independence is carried throughout the system, extending from the sensor to the devices actuating the protective function. Physical separation is used to achieve separation of redundant transmitters. Separation of wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant protection channel

set. Redundant analog equipment is separated by locating modules in different protection rack sets. Each redundant channel set is energized from a separate Class 1E ac power source.

There are four separate process analog protection sets. Separation of redundant analog channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and analog protection cabinets to the redundant trains in the logic cabinet. Redundant analog channels are separated by locating modules in different protection sets. Since all equipment within any cabinet is associated with a single protection set, there is no requirement for separation of wiring and components within the cabinet.

In the nuclear instrumentation system, process systems, and the solid-state protection system (SSPS), input cabinets where redundant channel instrumentation are physically adjacent, fire barriers, conduit, or wire duct is utilized and this ensures that a fire resulting from electrical failure in one channel would not propagate into redundant channels.

Independence of the logic trains is discussed in reference 2. Two reactor trip breakers are actuated by two separate logic matrices which interrupt power to the control rod drive mechanisms. The breaker main contacts are connected in series with the power supply so that opening either breaker interrupts power to all full length control rod drive mechanisms, permitting the full length rods to free fall into the core.

7.1.2.2.2.1 Reactor Trip System

A. Separate routing is maintained for the analog sensing signals, bistable output signals, and power supplies of the four basic RTS channel sets. Separation of these four channel sets is maintained from sensors to instrument racks to logic system cabinets.

B. Separate routing of the reactor trip signals from the redundant logic system cabinets is maintained, and in addition, they are separated (by spatial separation or by provision of barriers or by separate cable trays or wireways) from the four analog channel sets.

7.1.2.2.2.2 Engineered Safety Features Actuation System

A. Separate routing is maintained for the four basic sets of ESFAS analog sensing signals, bistable output signals, and power supplies. Separation is maintained from sensors to instrument cabinets to logic system input cabinets.

B. Separate routing of the ESFAS from the redundant logic system cabinets is maintained. In addition, they are separated by spatial separation, by provisions of barriers or by separate cable trays or wireways from the four analog channel sets.

C. Separate routing of control and power circuits associated with the operation of ESF equipment is required to retain redundancies provided in the system design and power supplies.

7.1.2.2.2.3 Instrumentation and Control Power Supply System

The separation criteria presented also apply to the power supplies for the load centers and busses distributing power to redundant components and to the control of these power supplies. Reactor trip system and engineered safety features actuation system analog circuits may be routed in the same wireways provided circuits have the same power supply train and channel set identified.

The physical identifications of safety-related equipment are given in paragraph 8.3.1.3.

The physical identifications of NSSS protection channel sets have been associated to the following separation groups:

NSSS Protection Channel Set	Separation Group See paragraph 8.3.1.3
I	A
II	B
III	C
IV	D

7.1.2.2.2.4 Electrical Separation

A. General Electrical Separation

Separation of redundant circuits conforms to the requirements of IEEE-384, Standard Criteria for Independence of Class 1E Equipment and Circuits.

Train A and Protection Set I do not require physical separation from each other except as described in paragraph B below.

B. Separation of Redundant (Class 1E) Circuits.

Separate routing is maintained for the four reactor protection/engineered safeguards channels. These channels are designated as I, II, III, and IV and include sensors, process and nuclear instrumentation cabinets, and provide inputs to the solid-state protection system.

Separate routing is maintained for the two redundant protection trains. These trains are designated A and B and include signals for reactor trip and safeguards initiation.

The safeguards actuation signals have physical separation from the four reactor protection/engineered safeguards channels and the reactor trip signals.

C. Separation of Post-Accident Monitoring (PAM) Signals

Post-accident monitoring signals from sensors to instrumentation cabinets are identified as Channels I, II, III, IV and are separated and routed in accordance with the requirements for reactor protection/engineered safeguards channel signals as described in paragraph B.

These signals are isolated at the output of the instrumentation cabinets and are routed to the main control room.

D. Cable Separation by Potential

Power and control conductors operating at potentials of 600 volts or less are not placed in cable trays with conductors operating at potentials of more than 600 volts.

For Class 1E circuits, analog or other low level signal conductors (potentials less than 100 volts), are not routed in cable trays containing power or control cables (potentials greater than 100 volts).

Analog or other low level signal conductors for non-Class 1E circuits are not routed in cable trays with conductors with potentials that exceed 120V ac and 125V dc.

These considerations are in conformance with the interface requirements established in reference 3.

Additional cable separation by potential requirements are provided in subparagraph 8.3.1.4.1.

E. Other Electrical Separation Requirements

Pressurizer Backup Heaters - The two redundant groups of pressurizer backup heaters used for maintaining the plant at hot shutdown obtain power from separate standby diesel generators.

Nuclear Instrumentation Systems (NIS) - All cables between the NIS cabinets and the sensors, including those associated with pre-amplifiers, are contained in four conduit groups: One group for each redundant protection channel. Only NIS cables are contained in these conduits. The minimum separation from the conduits and containment penetrations to electrical noise sources such as power sources of 120V ac, and higher, or circuits with switched loads such as relays or SCRs is 2 feet, or is suitably

shielded to reduce noise to an equivalent value. The minimum separation between 4160V cables and the above power cables is 6 feet or is suitably shielded to reduce noise to an equivalent value.

Non-Class 1E Circuits - Circuits not classified as reactor protection/engineered safeguards channels, reactor trip signals, safeguards actuation signals or post-accident monitoring signals are considered non-Class 1E circuits and are separated from redundant circuits as required by IEEE-384.

7.1.2.2.3 Separation of NSSS Instrument Lines (Sensor to Process Connections)

The minimum separation between redundant instrument impulse lines is at least 10 inches (46 centimeters) in air in both horizontal and vertical directions in non-missile or jet stream areas and is maintained from its starting point at the root valves to the vicinity of the instrument. If this separation is not possible, then a suitable barrier shall be used and it shall extend at least 1 inch (25 millimeters) beyond the line of sight between the redundant impulse lines.

Where potential missiles can be identified, additional separation, missile shields, and/or barriers shall be used.

Where redundant instrument impulse lines penetrate a wall or floor, the penetrations are separated by a minimum distance of 10 inches in non-missile or jet stream areas. If separate penetrations are not possible for the multiple lines, then they may be run through one common penetration provided that the following conditions are met:

A. Redundant instrument impulse lines shall be protected from postulated effects of failure of one another by a suitable barrier, such as a guard pipe.

B. A missile shield shall be provided around the instrument impulse lines until the minimum separation distance of 10 inches is achieved between the different redundant impulse lines.

In those few places where it is impractical to provide redundant taps (i.e., on an elbow flow element for example), the signal tap shall be protected from credible sources of common mode damage, and the "split" to redundant impulse lines shall be as close as possible to the process.

Pipe whip caused by nearby fluid systems piping shall be considered a credible event for all adjacent lines as required by the criteria described in subsection 3.6.1. Protection against adjacent pipe whip may be accomplished by restraining the adjacent pipe or by shielding the impulse line.

7.1.2.2.4 Fire Protection

For electrical equipment within the NSSS scope of supply, the NSSS supplier specifies non-combustible or fire-retardant material and conducts vendor-supplied specification reviews of this equipment which include assurance that materials will not be used which may ignite or explode from an electrical spark, flame, or from heating, or will independently support combustion. These reviews also include assurance of conservative current carrying capacities for all instrument cabinet wiring, which precludes electrical fires resulting from excessive over-current (I^2R) losses. For example, wiring used for instrument cabinet construction has teflon or tefzel insulation and will be adequately sized based on current carrying capacities set forth by ICEA and NEMA Standards. Braided sheathed material is non-combustible.

Additional details of fire protection, including the fire protection considerations for BOP electrical equipment and early warning protection system, are provided in subsection 9.5.1.

Panels not in the NSSS scope of supply are required to meet the following conditions:

A. All panel materials used, including terminal blocks, raceways, wireways, wire cleats, cable ties, and receptacles, shall not support combustion.

B. Paints and/or other applied surface preparations shall contribute minimally relative to the total combustible potential of materials or components in or on the panels. No preparation or material shall release toxic gases or dense smoke or propagate flames when heated or exposed to open flames. No material shall be of polyvinyl-chloride.

7.1.2.3 Physical Identification of Safety-Related Equipment

There are four separate protection sets identifiable with process equipment associated with the reactor trip and ESFAS. A protection set may be comprised of more than a single

process equipment cabinet. The color coding of each process equipment rack nameplate coincides with the color code established for the protection set of which it is a part. Redundant channels are separated by locating them in different equipment cabinets. Separation of redundant channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and equipment cabinets to the redundant trains in the logic racks. The solid-state protection system input cabinets are divided into four isolated compartments, each serving one of the four redundant input channels. Horizontal, 1/8-inch thick solid steel barriers, coated with fire-retardant paint, separate the compartments. Four, 1/8-inch thick solid steel, vertical wireways coated with fire-retardant paint enter the input cabinets. The wireway for a particular compartment is open only into that compartment so that flame could not propagate to affect other channels. A diagram of the input cabinet is given in figure 7.1-2.

At the logic racks the protection set color coding for redundant channels is clearly maintained until the channel loses its identity in the redundant logic trains. The color coded nameplates described below provide identification of equipment associated with protective functions and their channel set association:

Protection Set (Channel)	Color Coding
I or A	Red
II or B	Green
III or C	Yellow
IV or D	Blue

All non-cabinet mounted protective equipment and components are provided with an identification tag or nameplate. Small electrical components such as relays have nameplates on the enclosure which houses them. All cables are numbered with identification tags. In all areas, cable trays and conduits containing redundant circuits shall be identified using permanent markings. The purpose of such markings is to facilitate cable routing identification for future modification or additions. Positive permanent identification of cables and/or conductors shall be made at all terminal points. There are also identification nameplates on the input compartment doors of the solid-state protection system.

7.1.2.4 Conformance to Regulatory Guide 1.11 (Safety Guide 11), Instrument Lines Penetrating Primary Reactor Containment

Regulatory Guide 1.11 is discussed in appendix 3A.

7.1.2.5 Requirements for Periodic Testing Conformance to Regulatory Guide 1.22 (Safety Guide 22), Periodic Testing of Protection System Actuation Functions

Periodic testing of the reactor trip and ESFAS is described in subsections 7.2.2 and 7.3.2. Testing complies with Regulatory Guide 1.22, Periodic Testing of Protection System Actuation Functions, and IEEE 338, Standard Criteria for the Periodic Testing of Nuclear Power Generating Station Class iE Power and Protection Systems.

The surveillance requirements of ITS, ensure that the system functional operability will be maintained comparable to the orignal design standards. Periodic testing shall be conducted at the intervals specified in ITS Chapter 1 3.3.1 for reactor trip, ITS Chapter 1 3.3.2 for ESF actuation, and in ITS Chapter 1 3.3.3 for post-accident monitoring. Sensors will be demonstrated adequate for the design by test-reports, analysis, operating experience, or by suitable type testing. The nuclear instrumentation system detectors are excluded since delays attributable to them are not degradable. | S48 | S48

Where the ability of a system to respond to a bona fide accident signal is intentionally bypassed for the purpose of performing a test during reactor operation, each bypass condition is automatically indicated to the reactor operator in the main control room by a separate annunciator for the train in test. Test circuitry does not allow two trains to be tested at the same time so that extension of the bypass condition to the redundant system is prevented.

The actuation logic for the reactor trip and ESFAS is tested as described in sections 7.2 and 7.3. As recommended by Regulatory Guide 1.22, where actuated equipment is nat tested during reactor operation it has been determined that:

A. There is no practicable system design that would permit operation of the equipment without adversely affecting the safety or operability of the plant.

B. The probability that the protection system will fail to initiate the operation of the equipment is, and can be maintained, acceptably low without testing the equipment during reactor operation.

C. The equipment can routinely be tested when the reactor is shutdown.

The list of equipment that cannot be tested at full power so as not to damage equipment or upset plant operation is:

Manual actuation switches for system level actuation of protective functions

Reactor coolant pump breakers (trip)

Turbine trip

Main steam line isolation valves (close)

Main feedwater isolation valves (close)

Reactor coolant pump component cooling water isolation valves (close)

Reactor coolant pump seal water return valves (close)

Main feedwater control valves (close)

Main feedwater pump trip solenoids

2 Component cooling water surge tank vent valves (CLOSE)

The justification for not testing the above items at full power is discussed below.

A. Manual Actuation Switches - These would cause initiating plant upset and/or reactor trip. It should be noted that the reactor trip function that is derived from the automatic safety injection signal is tested at power as follows:

1. The analog signals, from which the automatic safety injection signal is derived, is tested at power in the same manner as the other analog signals and is described in subparagraph 7.2.2.2.3.10. The processing of these signals in the solid-state protection system (SSPS) wherein their channel orientation converts to a logic train orientation is tested at power by the built-in semi-automatic test provisions of the SSPS. The reactor trip breakers are tested at power as discussed in subparagraph 7.2.2.2.3.10.

B. Tripping of Reactor Coolant Pump Breakers

For credible frequency decay rates (less than 6.8 Hz/sec) the reactor coolant pumps are not required to be tripped.

Since opening of the reactor coolant pump breakers are not assumed for the accident analysis, and since testing them at power would cause plant upset, they do not need to be tested at power.

C. Turbine Tripping of the turbine can be tested at power up to and including actuation of individual dump fluid solenoids. Since two solenoids are required to actuate simultaneously to trip the turbine, each solenoid can be individually tested at power without tripping the turbine and upsetting the plant.

The generation of reactor trip from turbine trip is a testable function at power (similar to the other reactor trip generated from analog channels developing a bistable (on-off output) as follows:

1. The signal derived from the auto stop or pressure switch may be testable at power by exercising the switches one at a time by means of observance of local procedures at full power.

2. The position signal derived from the turbine steam stop valves is tested at reduced load by means of observance of local procedures when the functional tests of the steam inlet valves are performed on a one-valve-at-a-time basis.

D. Closing the Main Steam Line Isolation Valves - Main steam isolation valves are routinely tested during refueling outages. Testing of the main steam isolation valves to full stroke closure at power is not practical. As the plant power is increased, the core average temperature is programmed to increase. If the valves are closed under these elevated temperature conditions, the steam pressure transient would unnecessarily operate the steam generator relief valves and possibly the steam generator safety valves. The steam pressure transient produced would cause shrinkage in the steam generator level, which would cause the reactor to trip on low-low steam generator water level. Testing during operation will decrease the operating life of the valve.

Based on the above identified problems incurred with periodic full stroke closure testing of the main steam line isolation valves at power, and since, 1) no practical system design will permit operation of the valves without adversely affecting the safety or operability of the plant, 2) the probability that the protection system will fail to initiate the actuated equipment is acceptably low due to test up to final actuation, and 3) these valves will be routinely

tested during refueling outages. the proposed resolution meets the guidelines of Section D.4 of Regulatory Guide 1.22. Partial stroke testing is discussed in section 10.3.

E. Closing the Feedwater Isolation Valve - The feedwater Isolation valves are routinely tested during refueling outages. Periodic testing of these feedwater isolation valves. closing them completely or partially at power. would induce steam generator water level transients and oscillations which would trip the reactor. These transient conditions would be caused by perturbing the feedwater flow and pressure conditions necessary for proper operation of the feedwater pump control system and the steam generator water level control system.

Based on these identified problems incurred with periodic testing of the feedwater isolation valves at power. and since 1) no practical system design will permit operation of these valves without adversely affecting the safety or operability of the plant. 2) the probability that the protection system will fail to initiate the activated equipment is acceptably low due to testing up to final actuation. and 3) these valves will be routinely tested during refueling outages. the proposed resolution meets the guidelines of Section D.4 of Regulatory Guide 1.22.

F. Reactor Coolant Pump Component Cooling Water Return Isolation Valves (Close) - Component cooling water supply and return containment isolation valves are routinely tested during refueling outages. Testing of these valves while the reactor coolant pumps are operating introduces an unnecessary risk of costly damage to all the reactor coolant pumps. Loss of component cooling water to these pumps is of economic consideration only.

The reactor coolant pumps will not seize due to complete loss of component cooling. Information from the pump manufacturer indicates that the bearing babbitt would eventually break down but not so rapidly as to overcome the inertia of the flywheel. If the pumps are not stopped approximately 10 minutes after component cooling water is isolated. pump damage could be incurred.

Additional containment penetrations and containment isolation valves introduce additional unnecessary potential pathways for radioactive leakage following a postulated accident. Also. since the component cooling water flow rates and temperatures are about equal

during both plant power operation and plant refueling. periodic tests of these valves during a refueling outage would duplicate accident conditions.

Additionally, possibility of failure of containment isolation is remote because an additional failure of the pressure fluid system in addition to failure of both isolation valves would have to occur to open a path through the containment.

Based on the above described potential reactor coolant pump damage and with periodic testing of the component cooling water containment isolation valves at power, the duplication of at-power operating conditions during refueling outages, and since 1) no practical system design will permit operation of these valves without adversely affecting the safety or operability of the plant, 2) the probability that the protection system will fail to initiate the activated equipment is acceptably low due to the testing up to final actuation, and 3) these valves will be routinely tested during refueling outages when the reactor coolant pumps are not operating, the proposed resolution meets the guidelines of Section D.4 of Regulatory Guide 1.22.

G. Seal Water Return Valves (Close) - Seal return line isolation valves are routinely tested during refueling outages. Closure of these valves during operation would cause the safety valve to lift, with the possibility of valve chatter. Valve chatter would damage this safety valve. Testing of these valves at power would cause equipment damage. Therefore, these valves will be tested during scheduled refueling outages. As above, additional containment penetrations and containment isolation valves introduce additional unnecessary potential pathways for radioactive release following a postulated accident. Thus, the guidelines of Section D.4 of Regulatory Guide 1.22 are met.

H. Closing the Feedwater Control Valves - These valves are routinely tested during refueling outages. To close them at power would adversely affect the operability of the plant. The verification of operability of feedwater control valves at power is assured by confirmation of proper operation of the steam generator water level system. The actuation signals to the solenoids, which provides the closing function, is periodically tested at power as discussed in subparagraph 7.3.2.2.5. The operability of the slave relay

which actuates the solenoid, which is the actuating device, is verified during this test. Although the actual closing of these control valves is blocked when the slave relay is tested, all functions are tested to assure that no electrical malfunctions have occurred which could defeat the protective function. It is noted that the solenoids work on the de-energize-to-actuate principle, so that the feedwater control valves will fail closed upon either the loss of electrical power to the solenoids or loss of air pressure.

Based on the above, testing of the isolating function of feedwater control valves meets the guidelines of Section D.4 of Regulatory Guide 1.22.

I. Main Feedwater Pump Trip Solenoids - The containment integrity analysis does not assume tripping of the feedwater pumps: they are not considered safety-related and require no periodic testing. These functions are routinely tested during refueling outages.

J. Component Cooling Water Surge Tank Vent Valve

2

The vent valve acts as anticipatory pressure relief valve for its respective component cooling water surge tank during normal plant operation.
This valve was procured as an active valve and will fail-close upon failure of the control signal.
Failure of this valve to open will not jeopardize the performance of the system and the tank meets the code requirement since the spring loaded relief valve is installed to provide overpressure protection.
The safety injection signal serves to positive close the component cooling water surge tank vent valve during accident condition.
Testing of the valve in its respective component cooling water surge tank at power could potentially cause system upset, therefore testing can be performed during refueling outages.

7.1.2.6 Conformance with Regulatory Guide 1.29, Revision 1 (Safety Guide 29), Seismic Design Classifications

Regulatory Guide 1.29 is discussed in appendix 3A.

7.1.2.7 Conformance with Regulatory Guide 1.30 (Safety Guide 30), Quality Assurance Requirements for the Installation, Inspections, and Testing of Instrumentation and Electric Equipment

Regulatory Guide 1.30 is discussed in appendix 3A and chapter 17.

7.1.2.8 Conformance with Regulatory Guide 1.32, Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants

Regulatory Guide 1.32 is discussed in appendix 3A.

7.1.2.9 Conformance with Regulatory Guide 1.40, Qualification Tests of Continuous Duty Motors Installed Inside the Containment of Water Cooled Nuclear Power Plants

Conformance with Regulatory Guide 1.40 is discussed in appendix 3A.

7.1.2.10 Conformance with Regulatory Guide 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems

Conformance with Regulatory Guide 1.47 is discussed in appendix 3A.

Bypass/inoperability indication is in agreement with Regulatory Guide 1.47 with the following clarification:

A. An indicator of bypass/inoperability will be provided for redundant or diverse portions of each safety system. (Bypass includes any deliberate action which renders a safety system inoperable.)

B. Only permanently installed electrical control devices in accessible locations are considered for bypassing a safety system.

The term "permanently installed" does not include the portable handle required to rack out a circuit breaker. Devices within the containment or devices requiring an administratively controlled key to operate are not considered accessible. The term "control devices" applies to equipment intended to be acted upon by an operator, such as control switches. It does not include equipment which might be manipulated by prodding, such as relays.

C. Bypass of redundant portions of ESF support systems warrants indicators which must be differentiated from safety system bypass indicators. Support system bypass shall actuate safety system bypass indicators in a manner which reflects the impact of the support system on the safety system.

7.1.2.11 Conformance to Regulatory Guide 1.53, Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems and IEEE Standard 379

Conformance with Regulatory Guide 1.53 is discussed in appendix 3A.

The principles described in IEEE Standard 379 were used in the design of the Westinghouse protection system. The system complies with the intent of this standard and the additional guidance of Regulatory Guide 1.53. The formal analyses have not been documented exactly as outlined, although parts of such analyses are published in various documents such as the Fault Tree Analysis in reference 1.

The referenced topical report provides details of the analyses of the protection systems previously made to show conformance with single failure criterion set forth in Paragraph 4.2 of IEEE Standard 279. The interpretation of single failure criterion provided by IEEE Standard 379 does not indicate substantial differences with the interpretation of the criterion except in the methods used to confirm design reliability.

Established design criteria in conjunction with sound engineering practices form the bases for the protection systems. The reactor trip and ESFAS are each redundant safety systems. The required periodic testing of these systems will disclose any failures or loss of redundancy which could have occurred in the interval between tests, thus ensuring the availability of these systems.

Protection system design, of BOP supplied portions, will conform with Regulatory Guide 1.53 and IEEE Standard 379 as interpreted below. The required failure mode analysis, which will include channel power supplies, BOP protection system logic, and the actuator system, are provided in section 7.3.

A. As stated in regulatory position C-1, due to the trial use status of source document IEEE 379, departure from certain provisions may occur.

B. with regard to regulatory position C-2, the protection system as defined by IEEE 279 incorporates the capabilities for test and calibration as set forth in Paragraphs 4.9 and 4.10 of IEEE 279.

   Final actuation devices (as defined by IEEE 379) are capable of periodic testing in accordance with Regulatory Guide 1.22. The final actuation devices which cannot be fully tested during reactor operation (for reasons stated in regulatory positions 4a through 4c of Regulatory Guide 1.22) can be subjected to a partial test with the unit on line and to full operational testing during reactor shutdown. These devices are tested and discussed in paragraph 7.1.2.5.

   Taken as a whole, the operability of all active components necessary to achieve protective functions can be demonstrated via the testing program described above.

C. With regard to regulatory position C-3, single switches supplying signals to redundant channels are designed with at least 6 inches separation or suitable barriers between redundant circuits.

D. Compliance with single failure criteria can be verified based on a collective analysis of both the protective system defined in IEEE 279 and the final actuation devices or actuators defined in IEEE 379.

7.1.2.12 Conformance with Regulatory Guide 1.62, Manual Initiation of Protective Actions

Regulatory Guide 1.62 is discussed in subparagraph 7.3.2.2.7 and appendix 3A.

7.1.2.13 Conformance with Regulatory Guide 1.63, Electric Penetration Assemblies in Containment Structures for Water-Cooled Nuclear Power Plants

Regulatory Guide 1.63 is discussed in appendix 3A and chapter 8.

7.1.2.14 Conformance with Regulatory Guide 1.68, Preoperational and Initial Startup Test Programs for Water Cooled Power Reactors

Regulatory Guide 1.68 is discussed in appendix 3A and chapter 14.

7.1.2.15 Conformance with Regulatory Guide 1.73, Qualification Tests of Electric Valve Operators Installed Inside the Containment of Nuclear Power Plants

Regulatory Guide 1.73 is discussed in appendix 3A.

7.1.2.16 Conformance with Regulatory Guide 1.75, Physical Independence of Electric Systems

Regulatory Guide 1.75 is discussed in subparagraph 7.1.2.2.1, chapter 8, and appendix 3A.

7.1.2.17 Conformance with Regulatory Guide 1.80, Preoperational Testing of Instrument Air Systems

Regulatory Guide 1.80 is discussed in appendix 3A.

7.1.2.18 Conformance with Regulatory Guide 1.89, Qualification of Class 1E Equipment for Nuclear Power Plants

Regulatory Guide 1.89 is discussed in appendix 3A.

7.1.2.19 Conformance with Regulatory Guide 1.97, Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident

Regulatory Guide 1.97 is discussed in section 7.5 and appendix 3A.

7.1.2.20 Conformance with Regulatory Guide 1.105, Instrument Set Points

Regulatory Guide 1.105 is discussed in appendix 3A.

7.1.2.21 Conformance with Regulatory Guide 1.120, Fire Protection Guidelines for Nuclear Power Plants

Regulatory Guide 1.120 is discussed in appendix 3A and chapter 8.

7.1.2.22 Conformance with IEEE Standard 279, Criteria for Protection Systems for Nuclear Power Generating Systems

IEEE Standard 279 is discussed in sections 7.2, 7.3, 7.4, 7.5 and 7.6.

7.1.2.23 Conformance with IEEE Standard 308, Criteria for Class 1E Power Systems for Nuclear Power Generating Systems

IEEE Standard 308 is discussed in section 7.6 and 8.1.

7.1.2.24 Conformance with IEEE Standard 317, Electric Penetration Assemblies in Containment Structures for Nuclear Power Generating Stations

Electrical penetrations and conformance with IEEE Standard 317 is discussed in chapter 8.

7.1.2.25 Conformance with IEEE Standard 323, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

Environmental qualification of Class 1E electrical equipment, IEEE Standard 323 is discussed in section 3.11.

7.1.2.26 Conformance with IEEE Standard 334, Standard for Type Tests of Continuous Duty Class 1E Motors for Nuclear Power Generating Stations

Qualification of continuous duty Class 1E motors, IEEE Standard 334, is discussed in section 3.11.

7.1.2.27 Conformance with IEEE Standard 336, Installation, Inspection and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations

Installation, inspection, and testing for electrical equipment is discussed throughout this FSAR. A separately published QA manual provides a description of the quality assurance applied to the equipment. Conformance with IEEE Standard 336 is covered in the discussions of Regulatory Guide 1.30 in appendix 3A and in section 8.1. 51

7.1.2.28 Conformance to IEEE Standard 338, IEEE Standard Criteria for the Periodic Testing of Nuclear Power Generating Station Safety Systems

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

A. The surveillance requirements of the technical specifications for protection system ensure that the system functional operability is maintained comparable to the original design standards. Periodic tests at frequent intervals demonstrate this capability for the system, excluding sensors.

Sensors within the Westinghouse scope will be demonstrated adequate for this design by vendor testing, onsite tests in operating plants with appropriately similar design, or by suitable type testing. The nuclear instrumentation system detectors are excluded since they exhibit response time characteristics such that delays attributable to them are negligible in the overall channel response time required for safety.

For the periodic verification test program for sensors, refer to the technical specification. When finalized, technical specifications will require periodic verification testing on at least 18-month intervals.

Each test shall include at least one logic train such that both logic trains are tested at least once per 36 months and one channel per function such that all channels are tested at least once in every (18N months), where N is the total number of redundant channels in a specific protective function.

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

B. It is expected that the reliability goals specified in Paragraph 4.2 of IEEE Standard 338 (which are being developed by others on an industry generic basis) and adequacy of time intervals will be demonstrated at a later time.

C. The periodic time interval discussed in Paragraph 4.3 of IEEE Standard 338 and specified in the plant technical specifications is conservatively selected to assure that equipment associated with protection functions has not drifted beyond its minimum performance requirements. If any protection channel appears to be marginal or requires more frequent adjustments due to plant condition changes, the time interval will be decreased to accommodate the situation until the marginal performance is resolved.

D. The test interval discussed in paragraph 6.5 of IEEE Standard 338 is developed primarily on past operating experience and modified if necessary to assure that system and subsystem protection is reliably provided.

Analytic methods for determining reliability are not used to determine test interval.

Based on the scope definition given in IEEE Standard 338, no other systems described in chapter 7 are required to comply with this standard.

7.1.2.29 Conformance with IEEE Standard 344, Recommended Practices for Seismic Qualification of Class 1E Electrical Equipment for Nuclear Power Generating Stations

IEEE Standard 344 is discussed in section 3.10.

7.1.2.30 Conformance with IEEE Standard 379, Standard Application of the Single Failure Criteria to Nuclear Power Generating Station Class 1E Systems

IEEE Standard 379 is discussed in paragraph 7.1.2.11.

7.1.2.31 Conformance with IEEE Standard 382, Guide for Type Test of Class I Electric Valve Operators for Nuclear Power Generating Stations

Qualification of Class I electric valve operators, IEEE Standard 382, is discussed in section 3.11.

7.1.2.32 Conformance with IEEE Standard 384, Standard Criteria for Independence of Class 1E Equipment and Circuits

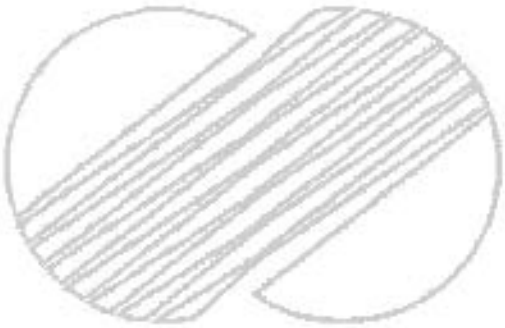
IEEE Standard 384 is discussed in chapter 8.

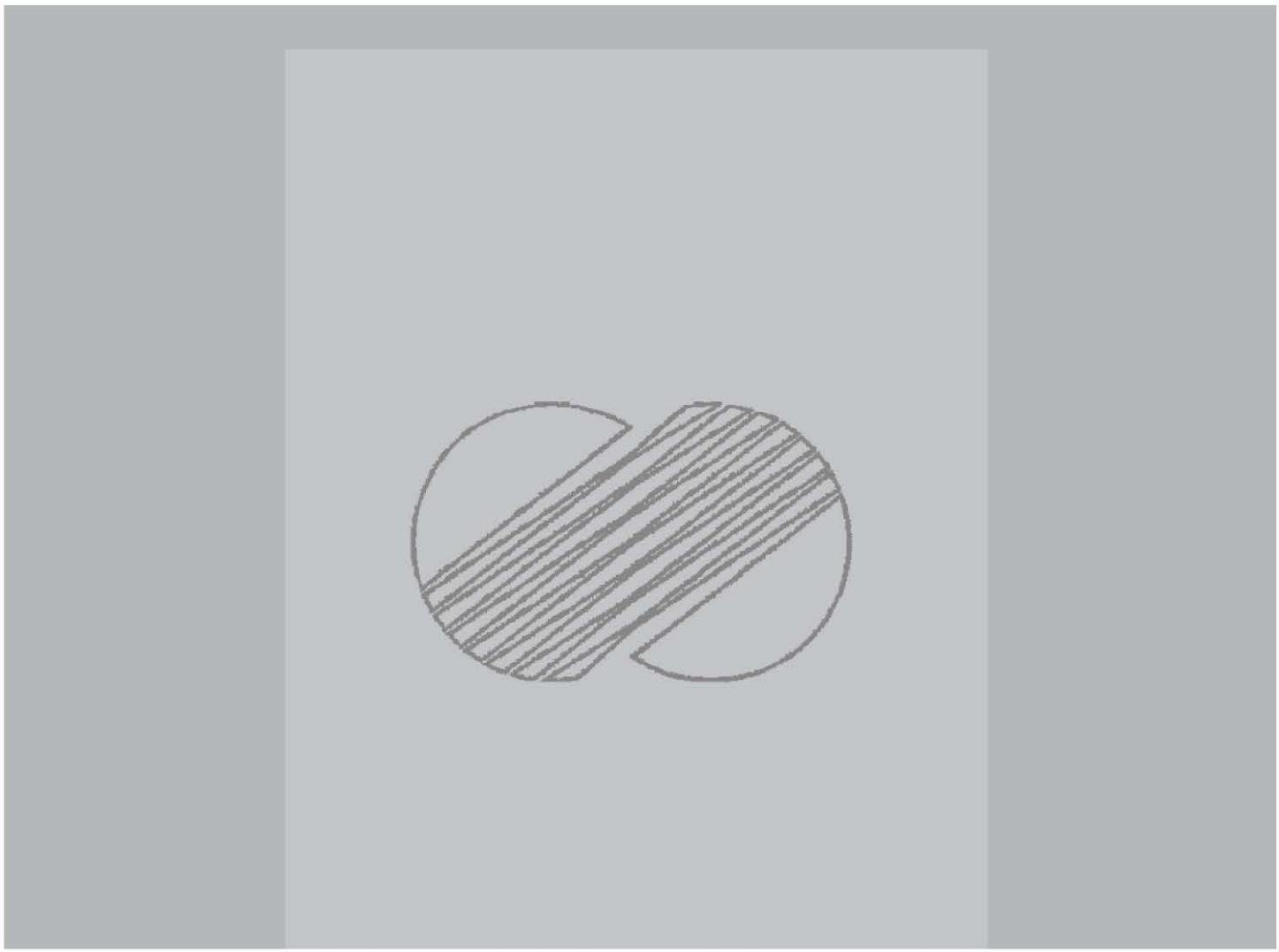
7.1.3 REFERENCES.

1. Gangloff, W. C. and Loftus, W. D., "An Evaluation of Solid-State Logic Reactor Protection in Anticipated Transients.'" WCAP-7706, February 1973.

2. Katz, D. N., "Solid-State Logic Protection System Description," WCAP-7672, May 1971.

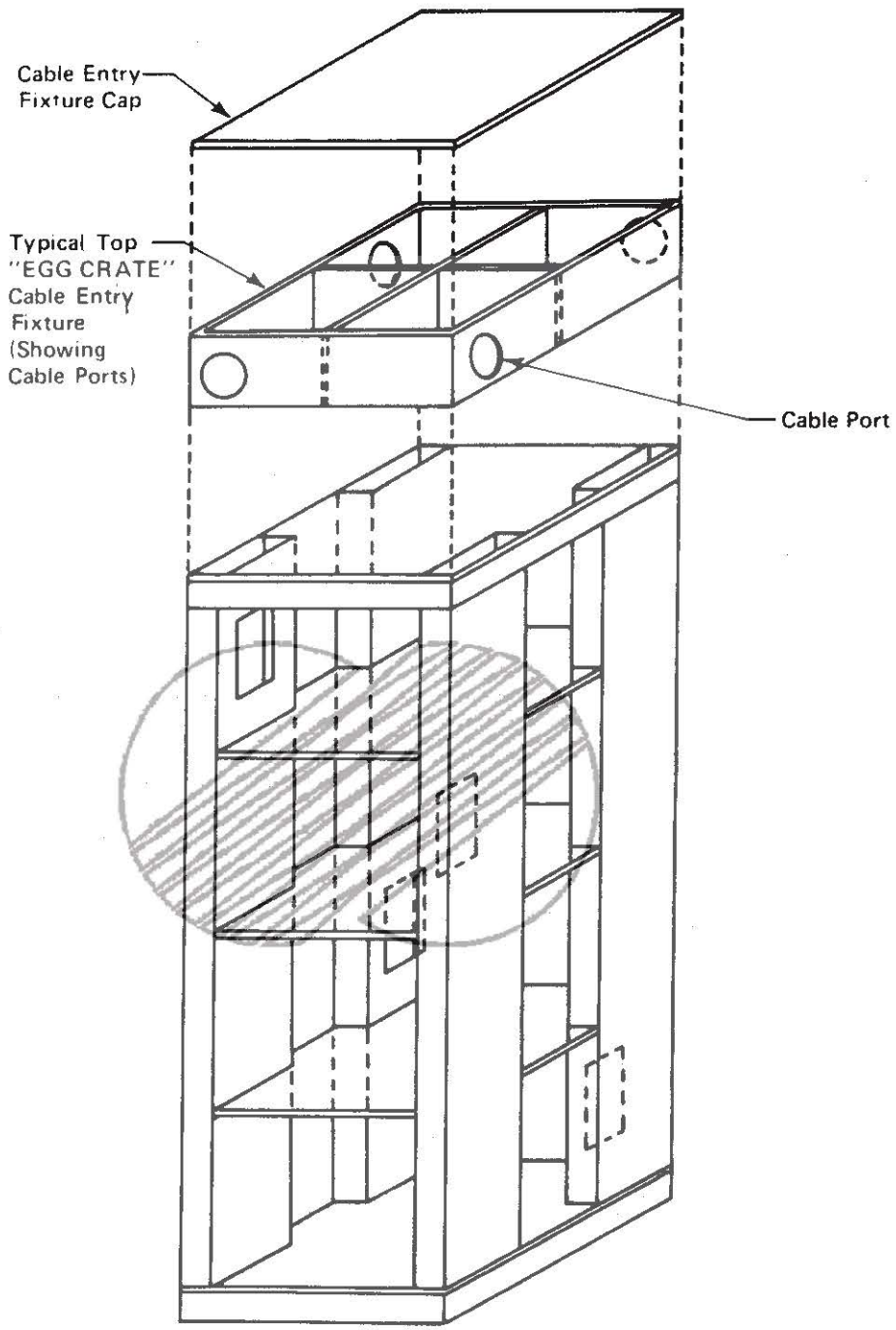
3. Siroky, R. M. and Marasco, F. W., "7300 Series Process Control System Noise Tests," WCAP-8892-A, June 1977.





KOREA ELECTRIC POWER CORPORATION
KOREA NUCLEAR UNITS 7 & 8
FSAR

PROTECTION SYSTEM BLOCK DIAGRAM
Figure 7.1-1



KOREA ELECTRIC POWER CORPORATION
KOREA NUCLEAR UNITS 7 & 8
FSAR

SSPS INPUT RELAY BAY
Figure 7.1-2

Table 7.1-1

INSTRUMENTATION SYSTEMS IDENTIFICATION (Sheet 1 of 3)

Systems or Categories	Section, Subsection, or Paragraph	Designer		Similar to Plant
		Westinghouse	Bechtel	KRN 3 & 4
Reactor Trip	7.2	x		x
Engineered Safety Features Actuation System	7.3			
Safety Injection System	7.3.1.1.4, 6.3	x		x
Main Steam and Feedwater Isolation	10.3 10.4.7 7.3.3.11	x		x
Containment Isolation	6.2.4, 7.3.3.9	x		x
Containment Heat Removal	6.2.2	x		x
Containment Combustible Gas Control	7.3.3.8		x	x
Containment Purge Isolation	7.3.3.4		x	x
Containment Spray	7.3.1.1.4.1	x		x

Table 7.1-1

INSTRUMENTATION SYSTEMS IDENTIFICATION (Sheet 2 of 3)

Systems or Categories	Section, Subsection, or Paragraph	Designer		Similar to Plant
		Westinghouse	Bechtel	KRN 3 & 4
Feedwater Isolation	7.3.1.1.4.1	X		X
Containment Fan Cooler	7.3.3.7		X	X
Fuel Building Emergency Ventilation	7.3.3.5		X	X
Control Room Emergency Ventilation	7.3.3.6		X	X
Auxiliary Feed-water Control	7.3.3.2	X	X	X
Diesel Generator Load Sequencer	7.3.1.1.4.2		X	X
Systems Required for Safe Shutdown				
Hot Shutdown	7.4	X		X
Cold Shutdown	7.4	X		X
Shutdown from Outside Control Room	7.4.1.3	X	X	X

Table 7.1-1

INSTRUMENTATION SYSTEMS IDENTIFICATION (Sheet 3 of 3)

Systems or Categories	Section, Subsection, or Paragraph	Designer		Similar to Plant
		Westinghouse	Bechtel	KRN 3 & 4
Safety-Related Display Instrumentation	7.5	X		X
Reactor Trip	7.2.2.2.3.20	X		X
Engineering Safety Features Actuation System	7.5	X	X	X
Other Instrumentation Systems Required for Safety				
Vital Instrument ac Power Supply	7.6.1 8.3.1.1.5		X	X
Residual Heat Removal Isolation Valves	7.6.2	X		X
Refueling Interlocks	7.6.3	X		X

(This page intentionally left blank)

Table 7.1-2

LISTING OF APPLICABLE CRITERIA (Sheet 2 of 11)

Criteria	Title	Discussed in:
1. General Design Criteria (GDC), Appendix A to 10 CFR Part 50		
GDC 1	Quality Standards and Records	3.1.2, 7, a separately published QA manual
GDC 2	Design Bases for Protection Against Natural Phenomena	3.1.2, 3.10, 3.11, 7.2.1.1.11
GDC 3	Fire Protection	3.1.2, 7.1.2.2.4, 9.5.1
GDC 4	Environmental and Missile Design Program	3.1.2, 3.11, 7.2.2.2.3.4
GDC 5	Sharing of Structures, Systems, and Components	3.1.2
GDC 10	Reactor Design	3.1.2, 7.2.2.2
GDC 12	Suppression of Reactor Power Oscillations	3.1.2, 15, 7.7
GDC 13	Instrumentation and Control	3.1.2, 7.3.1, 7.3.2, 7.7
GDC 15	Reactor Coolant System Design	3.1.2, 7.2.2.2.1
GDC 17	Electric Power Systems	3.1.2, 8, 7.6
GDC 19	Control Room	3.1.2, 7.4.1.3, 7.5
GDC 20	Protection System Functions	3.1.2, 7.2.2.1, 7.3.1.1, 7.3.2.2, 7.2.2.2

Table 7.1-2

LISTING OF APPLICABLE CRITERIA (Sheet 2 of 11)

Criteria	Title	Discussed in:
GDC 21	Protection System Reliability and Testability	3.1.2. 7.2.2. 7.3.1. 7.3.2
GDC 22	Protection System Independence	3.1.2. 7.1.2.2. 7.2.2.2. 7.3.1. 7.3.2
GDC 23	Protection System Failure Modes	3.1.2. 7.2.2.2. 7.3.1.1. 7.3.2.2. 7.7.2.2
GDC 24	Separation of Protection and Control Systems	3.1.2. 7s2.2.2. 7.3.1. 7.3.2
GDC 25	Protection System Requirements for Reactivity Control, Malfunctions	3.1.2. 7.3.2
GDC 26	Reactivity Control System Redundancy and Capability	3.1.2
GDC 27	Combined Reactivity Control Systems Capability	3.1.2. 7.3.1. 7.3.2.2. 15
GDC 28	Reactivity Limits	3.1.2. 7.3.1. 7.3.2.2. 15
GDC 29	Protection Against Anticipated Operational Occurrence	3.1.2. 7.2.2.1. 7.2.2.2
GDC 33	Reactor Coolant Makeup	3.1.2
GDC 34	Residual Heat Removal	3.1.2
GDC 35	Emergency Core Cooling	3.1.2. 7.3.2.2. 7.3.1.1.4

Table 7.1-2

LISTING OF APPLICABLE CRITERIA(Sheet 3 of 11)

Criteria	Title	Discussed in:
GDC 37	Testing of Emergency Core Cooling System	3.1.2, 7.3.2
GDC 38	Containment Heat Removal	3.1.2, 7.3.2
GDC 40	Testing of Containment Heat Removal System	3.1.2, 7.3.2.2
GDC 41	Containment Atmosphere Cleanup	3.1.2, 7.3.2
GDC 43	Testing of Containment Atmosphere Cleanup Systems	3.1.2, 7.3.2.2
GDC 44	Cooling Water	3.1.2
GDC 46	Testing of Cooling Water System	3.1.2, 7.3.2.2
GDC 50	Containment Design Basis	3.1.2
GDC 54	Piping Systems Penetrating Containment	3.1.2, 6.2.4
GDC 55	Reactor Coolant Pressure Boundary Penetrating Containment	3.1.2, 6.2.4
GDC 56	Primary Containment Isolation	3.1.2, 6.2.4
GDC 57	Closed Systems Isolation Valves	3.1.2, 6.2.4

Table 7.1-2

LISTING OF APPLICABLE CRITERIA (Sheet 4 of 11)

Criteria	Title	Discussed in:
2. Institute of Electrical and Electronics Engineers (IEEE) Standards		
IEEE Std 279 (ANSI N42.7-1971)	Criteria for Protection Systems for Nuclear Power Generating Systems	7.1.2.22, 7.2, 7.3, 7.4, 7.5, 7.6
IEEE Std 308 - 1978	Criteria for Class 1E Power Systems for Nuclear Power Generating Stations	7.6, 8.1 7.1.2.23
IEEE Std 317 - 1976	Electric Penetration Assemblies in Containment Structures for Nuclear Power Generating Stations	8.1, 7.1.2.24
IEEE Std 323 - 1974	IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations	3.11, 7.1.2.25
IEEE Std 334 - 1974	Standard for Type Tests of Continuous-Duty Class 1E Motors for Nuclear Power Generating Stations	3.11, 7.1.2.26

Table 7.1-2

LISTING OF APPLICABLE CRITERIA (Sheet 5 of 11)

Criteria	Title	Discussed in:
IEEE Std 336 - 1977 (ANSI N45.2.4 1972)	Installation, Inspection and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations	a separately published QA manua. 7.1.2.27
IEEE Std 338 - 1977	Criteria for the Periodic Testing of Nuclear Power Generating Station Class 1E Power and Protection Systems	7.1.2.28. 7.2.2. 7.3.2
IEEE Std 344 - 1975	Seismic Qualification of Class 1E Electrical Equipment for Nuclear Power Generating Stations	3.10. 7.1.2.29
IEEE Std 379 - 1977(ANSI N41.2)	Standard Application of the Single Failure Criteria to Nuclear Power Generating Station Class 1E Systems	7.1.2.11. 7.1.2.30
IEEE Std 382 - 1972	Type Test of Class 1E Electric Valve Operators	3.11. 7.1.2.31
IEEE Std 384 - 1977(ANSI N41.14)	Trial Use Standard Criteria for Independence Class 1E Equipment and Circuits	7.1.2.32. 8

51

Table 7.1-2

LISTING OF APPLICABLE CRITERIA (Sheet 6 of 11)

Criteria	Title	Discussed in:
3. Regulatory Guides (RG)	(See Appendix 3A)	
RG 1.6	Independence Between Redundant Standby (Onsite) Power Sources and Between Their Distribution Systems	Appendix 3A, 8.3.1.3
RG 1.7	Control of Combustible Gas Concentration in Containment Following a Loss-of-Coolant Accident	Appendix 3A, 6.2.5
RG 1.11	Instrument Lines Penetrating Primary Reactor Containment	Appendix 3A, 6.2.4.2, 7.3.1.1.2
RG 1.22	Periodic Testing of Protection System Actuation Functions	7.1.2.5, 7.2.2.2.3.2, 7.3.2.2
RG 1.29	Seismic Design Classification	Appendix 3A, 7.5.2.2.2.1
RG 1.30	Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment	Appendix 3A, a separately published QA manual.
RG 1.32	Criteria for Safety Related Electric Power Systems for Nuclear Power Plants.	Appendix 3A, 8

Table 7.1-2

LISTING OF APPLICABLE CRITERIA (Sheet 7 of 11)

Criteria	Title	Discussed in:
RG 1.40	Qualification Tests of Continuous Duty Motors Installed Inside the Containment of Water Cooled Nuclear Power Plants	Appendix 3A
RG 1.45	Reactor Coolant Pressure Boundary Leakage Detection Systems	Appendix 3A, 5.2.5
RG 1.47	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems	Appendix 3A, 7.1.2.10, 7.5.2.3.1
RG 1.53	Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems	Appendix 3A, 7.1.2.11
RG 1.62	Manual Initiation of Protection Actions	Appendix 3A, 7.3.2.2.7, 7.2.2.2.3.17
RG 1.63	Electric Penetration Assemblies in Containment Structures for Light Water Cooled Nuclear Power Plants	Appendix 3A, 8.3.1.4.1.3
RG 1.68	Initial Test Programs for Water Cooled Reactor Power Plants	Appendix 3A, 14.2

Table 7.1-2

LISTING OF APPLICABLE CRITERIA (Sheet 8 of 11)

Criteria	Title	Discussed in:
RG 1.70	Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Rev. 3	1. Appendix 3A
RG 1.73	Qualification Test of Electric Valve Operators Installed Inside the Containment	3.11.2. Appendix 3A
RG 1.75	Physical Indepen-dence of Electric Systems	Appendix 3A. 7.1.2.2.1. 8.3.1.3
RG 1.80	Preoperational Testing of Instru-ment Air System	Appendix 3A
RG 1.89	Qualification of Class 1E Equipment for Nuclear Power Plants	3.11. Appendix 3A
RG 1.95	Protection of Nuclear Power Plant Control Room Opera-tors Against an Accidental Chlorine Release	Appendix 3A
RG 1.97	Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident	7.5
RG 1.100	Seismic Qualifica-tion of Electric Equipment for Nuclear Power Plants	3.10.2

Table 7.1-2

LISTING OF APPLICABLE CRITERIA (Sheet 9 of 11)

Criteria	Title	Discussed in:
RG 1.105	Instrument Set Points	Appendix 3A. 7.1.2.1.9
RG 1.106	Thermal Overload Protection for Electrical Motors on Motor-Operated Valves	Appendix 3A. 8.3.1
RG 1.118	Periodic Testing of Electrical Power and Protection Systems	Appendix 3A. 7.1.2.28
RG 1.120	Fire Protection Guidelines for Nuclear Power Plants	Appendix 3A. 7.6.9. 9.5.1
4. Branch Technical Positions (BTP) EICSB		
BTP EICSB 3	Isolation of Low Pressure Systems from the High Pressure Reactor Coolant System	5.4.7.2.4. 7.6.2
BTP EICSB 4	Requirements on Motor-Operated Valves in the ECCS Accumulator Lines	6.3.2.2.15. 7.6.4
BTP EICSB 5	Scram Breaker Test Technical Specification	ITS Chapter 1 Table 3.3.1-1

Table 7.1-2

LISTING OF APPLICABLE CRITERIA (Sheet 10 of 11)

Criteria	Title	Discussed in:
BTP EICSB 9	Definition and Use of "Channel-Calibration"-Technical Specifications	ITS Chapter 1 Table 3.3.1-1
BTP EICSB 13	Design Criteria for Auxiliary Feedwater Systems	7.3.3.2, 10.4.9
BTP EICSB 14	Spurious Withdrawal of Single Control Rods in Pressurized Water Reactors	15.8
BTP EICSB 18	Application of the Single Failure Criteria to Manually Controlled Electrically-Operated Valves	7.3.2.2.1
BTP EICSB 20	Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode	6.3
BTP EICSB 21	Guidance for Application of Reg. Guide 1.47	Appendix 3A

Table 7.1-2

LISTING OF APPLICABLE CRITERIA (Sheet 11 of 11)

Criteria	Title	Discussed in:
BTP EICSB 22	Guidance for Application Guide 1.22	Appendix 3A
BTP EICSB 23	Qualification of Safety-Related Display Instrumentation for Post-Accident Condition Monitoring and Safe Shutdown	7.5
BTP EICSB 24	Testing of Reactor Trip System and Engineered Safety Feature Actuation System Sensor Response Times	7.1.2.5
BTP EICSB 25	Guidance for the Interpretation of General Design Criterion 37 for Testing the Operability of the Emergency Core Cooling System as a Whole	ITS Chapter 1 3.5
BTP EICSB 26	Requirements for System Anticipatory Trips	7.2, 7.7
BTP EICSB 27	Design Criteria for Thermal Overload Protection for Motors of Motor-Operated Valves	8.3.1.1.2.11

846

7.2 REACTOR TRIP SYSTEM

7.2.1 DESCRIPTION

7.2.1.1 System Description

The reactor trip system automatically prevents operation of the reactor in an unsafe region by shutting down the reactor whenever the limits of the safe region are approached. The safe operating region is defined by several considerations such as mechanical/hydraulic limitations on equipment, and heat transfer phenomena. Therefore, the reactor trip system maintains surveillance on process variables which are directly related to equipment mechanical limitations, such as pressure, pressurizer water level (to prevent water discharge through safety valves), and variables which directly affect the heat transfer capability of the reactor (e.g., flow and reactor coolant temperatures). Other parameters utilized in the reactor trip system are calculated from various process variables. In any event, whenever a direct process or calculated variable exceeds a setpoint, the reactor will be shut down in order to protect against either gross damage to fuel clad or loss of system integrity which could lead to release of radioactive fission products into the containment.

The following systems make up the reactor trip system (references 1, 2, and 3 provide additional background information on the systems):

A. Process Instrumentation and Control System[1]

B. Nuclear Instrumentation System[2]

C. Solid-State Logic Protection System[3]

D. Reactor Trip Switchgear

E. Manual Actuation Circuit.

Functional diagrams, figure 7.2-1, depict the reactor trip functions as well as associated functions. Reference is made in the text as necessary.

The reactor trip system consists of sensors which, when connected with analog circuitry consisting of two to four redundant channels, monitor various plant parameters: and digital circuitry, consisting of two redundant logic trains, which receives inputs from the analog protection channels to complete the logic necessary to automatically open the reactor trip breakers.

Each of the two trains, A and B, is capable of opening a separate and independent reactor trip breaker, RTA and RTB, respectively.

The two trip breakers in series connect three-phase ac power from the rod drive motor generator sets to the rod drive power cabinets, as shown in figure 7.2-1, sheet 2. During plant operation, a dc undervoltage coil on each reactor trip breaker holds a trip plunger out against its spring, allowing the power to be available at the rod control power supply cabinets. For
3 reactor trip, a loss of dc voltage to the undervoltage coil as well as energitation of the shunt trip coil, releases the trip plunger and trips open the breaker. When either of the trip breakers opens, power is interrupted to the rod drive power supply and the control rods fall, by gravity, into the core. The rods cannot be withdrawn until the trip breakers are manually reset. The trip breakers cannot be reset until the abnormal condition which initiated the trip is corrected. Bypass breakers BYA and BYB are provided to permit testing of the trip breakers.

7.2.1.1.1 Functional Performance Requirements

The reactor trip system automatically initiates reactor trip:

A. Whenever necessary to prevent fuel rod damage for an anticipated operational transient (Condition II)

B. To limit core damage for infrequent faults (Condition III)

C. So that the energy generated in the core is compatible with the design provisions to protect the reactor coolant pressure boundary for limiting fault conditions (Condition IV).

The reactor trip system initiates a turbine trip signal whenever a reactor trip is initiated. This prevents the reactivity insertion that would otherwise result from excessive reactor system cooldown and thus avoids unnecessary actuation of the engineered safety features (ESF) actuation system.

The reactor trip system provides for manual initiation of reactor trip by operator action in the control room.

7.2.1.1.2 Reactor Trips

The Various reactor trip circuits automatically open the reactor trip breakers whenever a condition monitored by the reactor trip systems reaches a preset level. To ensure a reliable system, high quality design, components, manufacturing, quality control, and testing are used. In addition to redundant channels and trains, the design approach provides a reactor trip system which monitors numerous system variables, therefore providing protection system functional diversity. The extent of this diversity has been evaluated for a wide variety of postulated accidents and is detailed in references 4 and 5.

Table 7.2-1 provides a list of reactor trips which are described below.

7.2.1.1.2.1 Nuclear Overpower Trips. The specific trip functions generated are as follows:

A. Power range high neutron flux trip

The power range high neutron flux trip circuit trips the reactor when two of the four power range channels exceed the trip setpoint.

There are two bistable amplifiers for overpower protection in each of four redundant nuclear instrumentation power range channels. Each has its own trip setting. The bistable trip setting (high setting) associated with monitoring the high end of the power range provides overpower protection and is never blocked. The bistable trip setting (low setting), which provides a more restrictive protection limit during startup and operation at low power level, can be manually blocked by the operator when two out of four power range channels indicate approximately 10 percent power (P-10). Three out of four channels below 10 percent automatically reinstate the trip (low setting) function. Refer to table 7.2-2 for a listing of all protection system interlocks.

B. Intermediate range high neutron flux trip

The intermediate range high neutron flux trip circuit trips the reactor when one out of the two intermediate range channels exceeds the trip setpoint. This trip, which provides protection during reactor startup, can be manually blocked if two out of four power range channels are above approximately 10 percent power (P-10). Three out of the four power range channels below this value automatically reinstate the intermediate range high neutron flux trip. The intermediate range channels (including detectors) are separate from the power range channels. The intermediate range channels can be individually bypassed at the nuclear instrumentation racks to permit channel testing during plant shutdown or prior to startup. This bypass action is annunciated on the control board.

C. Source range high neutron flux trip

The source range high neutron flux trip circuit trips the reactor when one of the two source range channels exceeds the trip setpoint. This trip, which provides

protection during reactor startup and plant shutdown. can be manually bypassed when one of the two intermediate range channels reads above the P-6 setpoint value and is automatically reinstated when both intermediate range channels decrease below the P-6 setpoint value. This trip is also automatically bypassed by two out of four logic from the power range protection interlock (P-10). This trip function can also be reinstated below P-10 by an administrative action requiring manual actuation of two control board mounted switches. Each switch will reinstate the trip function in one of the two protection logic trains. The source range trip point is set between the P-6 setpoint and the maximum source range power level. The channels can be individually bypassed at the nuclear instrumentation racks to permit channel testing during plant shutdown or prior to startup. This bypass action is annunciated on the control board.

105

D. Power range high positive neutron flux rate trip

This circuit trips the reactor when an abnormal rate of increase in nuclear power occurs in two out of four power range channels. This trip provides departure from nucleate boiling (DNB) protection against rod ejection accidents of low worth from mid-power and is always active.

E. **[DELETE]**

7.2.1.1.2.2 Core Thermal Overpower Trips. The specific trip functions generated are as follows:

A. Overtemperature ΔT trip

This trip protects the core against low DNBR and trips the reactor on coincidence as listed in table 7.2-1 with one set of temperature measurements per loop.

The setpoint for this trip is continuously calculated by analog circuitry for each loop by solving the following equation:

$$\Delta T\left(\frac{1+\tau_1 s}{1+\tau_2 s}\right)\left(\frac{1}{1+\tau_3 s}\right) \leq \Delta T_0\left\{K_1 - K_2\left(\frac{1+\tau_4 s}{1+\tau_5 s}\right)\left(T\left(\frac{1}{1+\tau_6 s}\right) - T'\right) + K_3(P-P') - f(\Delta\Phi)\right\}$$

where

$\frac{1+\tau_1 s}{1+\tau_2 s}$ = Lead−Lag compensator on measured ΔT

$\tau_1 \cdot \tau_2$ = Time constants utilized in the Lead−Lag controller

$\frac{1}{1+\tau_3 s}$ = Lag compensator on measured ΔT

τ_3 = Time constants utilized in the Lag compensator for ΔT

ΔT_0 = Indicated ΔT at rated thermal power, °F

K_1 = Preset bias

K_2 = Preset gain which compensator for piping and instrument time delay

$\frac{1+\tau_4 s}{1+\tau_5 s}$ = The function generated by the Lead−Lag controller for T_{avg} during compensation

$\tau_4 \cdot \tau_5$ = Time constants utilized in the Lead−Lag controller

T = Average temperature, °F

$\frac{1}{1+\tau_3 s}$ = Lag compensator on measured T_{avg}

T_δ = Time constants utilized in the measured T_{avg} Lag compenstor

T′ = Nominal T_{avg} at rated thermal power, °F

K_3 = Preset gain which compensates for the effect of pressure on the DNB limits

P = Pressurizer pressure, psig

p′ = Nominal RCS operating pressure, psig

s = Laplace transform operator, seconds^{-1}

f(ΔΦ) = A function of the neutron flux difference between upper and lower long ion chambers (refer to figure 7.2−2.)

A separate long ion chamber unit supplies the flux signal for each overtemperature ΔT trip channel.

Increases in ΔΦ beyond a predefined dead band result in a decrease in trip setpoint (refer to figures 7.2−2 and 7.2−3.)

The required one pressurizer pressure parameter per loop is obtained from separate sensors connected to three pressure taps at the top of the pressurizer. Refer to subparagraph 7.2.2.3.3 for an analysis of this arrangement.

Figure 7.2−1, sheet 5, shows the logic for overtemperature ΔT trip function.

B. Overpower △T trip

This trip protects against excessive power (fuel rod rating protection) and trips the reactor on coincidence as listed in table 7.2-1 with one set of temperature measurements per loop. The setpoint for each channel is continuously calculated using the following equation:

$$\Delta T\left(\frac{1+\tau_1 s}{1+\tau_2 s}\right)\left(\frac{1}{1+\tau_3 s}\right) \le \Delta T_0\left\{K_4 - K_5\left(\frac{\tau_7 s}{1+\tau_7 s}\right)T\left(\frac{1}{1+\tau_6 s}\right) + K_6\left[T\left(\frac{1}{1+\tau_6 s}\right) - T\right]\right.$$

where:

$\frac{1+\tau_1 s}{1+\tau_2 s}$ = Lead-Lag compensator on measured ΔT

τ_1, τ_2 = Time constants utilized in the Lead-Lag controller

$\frac{1}{1+\tau_3 s}$ = Lag compensator on measured ΔT

τ_3 = Time constants utilized in the Lag compensator for ΔT

ΔT_0 = Indicated ΔT at rated thermal power, °F

K_4 = A preset bias

K_5 = A preset gain which compensates for piping and instrument time delay

$\frac{\tau_7 s}{1+\tau_7 s}$ = The function generated by the rate-lag controller for T_{avg} dynamic compensator

τ_7 = Time constants utilized in the rate-Lag controller for T_{avg}

$\frac{1}{1+\tau_6 s}$ = Lag compensator on measured T_{avg}

τ_6 = Time constants utilized in the measured T_{avg} Lag compensator

K_6 = A preset gain which compensates for the change in density flow, and heat capacity of the water with temperature

T = Average temperature, °F

T° = Indicated T_{avg} at rated thermal power, °F

s = Laplace transform operator, second^{-1}

7.2.1.1.2.3 Reactor Coolant System Pressurizer and Water Level Trips. The specific trip functions generated are as follows:

A. Pressurizer low pressure trip

The purpose of this trip is to protect against low pressure which could lead to DNB. The parameter being sensed is reactor coolant pressure as measured in the pressurizer. Above P-7, the reactor is tripped when the pressurizer pressure measurements fall below preset limits. This signal is compensated to account for the fact that the measurement is in the pressurizer rather than in the core proper. This trip is blocked below P-7 because at low power it is not required to permit startup. The trip logic and interlocks are given in table 7.2-1.

The trip logic is shown in figure 7.2-1, sheet 6.

B. Pressurizer high pressure trip

The purpose of this trip is to protect the reactor coolant system against system overpressure and to prevent opening of the pressurizer safety valves.

The same sensors and transmitters used for the pressurizer low pressure trip are used for the high pressure trip except that separate bistables are used for trip. These bistables trip when uncompensated pressurizer pressure signals exceed preset limits on coincidence as listed in table 7.2-1. There are no interlocks or permissives associated with this trip function. This trip protects against overstressing the reactor coolant pressure boundary.

The logic for this trip is shown in figure 7.2-1, sheet 6.

C. Pressurizer high water level trip

This trip is provided as a backup to the high pressurizer pressure trip and serves to prevent water relief through the pressurizer safety valves and, therefore, provides for equipment protection. This trip is blocked below P-7 to permit startup. The coincidence logic and interlocks of pressurizer high water level signals are given in table 7.2-1.

The trip logic for this function is shown in figure 7.2-1, sheet 6.

7.2.1.1.2.4 Reactor Coolant System Low Flow Trips. These trips protect the core from DNB in the event of a loss of coolant flow situation. Figure 7.2-1, sheet 5, shows the logic for these trips. The means of sensing the loss of coolant flow are as follows:

A. Low reactor coolant flow

The parameter sensed is reactor coolant flow. Three differential pressure transmitters in each coolant loop are used to provide the status of reactor coolant flow. The basic function of this device is to provide information as to whether or not a reduction in flow has occurred. An output signal from two of the three bistables in a loop would indicate a low flow in that loop.

Above P-7, two of the three loop low flow signals will trip the reactor: above P-8, low flow in any one loop will cause a reactor trip.

The coincidence logic and interlocks are given in table 7.2-1. Trip logic for this function is shown in figure 7.2-1, sheet 5.

B. Reactor coolant pump undervoltage trip

This trip is required in order to protect against low flow which can result from loss of voltage to more than one reactor coolant pump motor (e.g., loss of offsite power or reactor coolant pump breakers opening).

There is one undervoltage sensing relay connected for each pump at the motor side of each reactor coolant pump breaker. These relays provide an output signal when the pump voltage goes below approximately 70 percent of rated voltage. Signals from these relays are time delayed to prevent spurious trips caused by short-term voltage perturbations. The coincidence logic and interlocks are given in table 7.2-1 and figure 7.2-1, sheet 5.

C. Reactor coolant pump underfrequency trip

This trip protects against low flow resulting from pump underfrequency: for example, a major power grid frequency disturbance.

The function of this trip is to trip the reactor for an underfrequency condition. The setpoint of the underfrequency relays is adjustable between 54 and 59 Hz.

There is one underfrequency sensing relay for each reactor coolant pump motor. Signals from relays connected to any two of the pump motors will trip the reactor if power is above P-7. Signals are time delayed to prevent spurious trips caused by short-term frequency perturbations.

Figure 7.2-1. sheet 5. shows the logic for the pump underfrequency trip.

7.2.1.1.2.5 Steam Generator Trips. The specific trip functions generated are as follows:

A. Low-low steam generator water level trip

This trip protects the reactor from loss of heat sink.

This trip is actuated on two out of the four low-low water level signals occurring in any steam generator.

The logic is shown in figure 7.2-1. sheet 7.

7.2.1.1.2.6 Reactor Trip on a Turbine Trip (Anticipatory). The reactor trip on a turbine trip is actuated by two-out-of three logic from low emergency trip fluid signals or by four-out-of-four signals generated by closure of the four turbine high pressure throttle(stop)valves. A turbine trip causes a direct reactor trip above P-8. The reactor trip on turbine trip provides additional protection and conservatism beyond that required. This trip is included as part of good engineering practice and prudent design. No credit is taken in any of the safety analyses (chapter 15) for this trip. | 2 | 31

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

One of the design bases considered in the protection system is the possibility of an earthquake. With respect to these contacts, their functioning is unrelated to a seismic event in that they are anticipatory to other diverse parameters which cause reactor trip. The contacts are closed during plant operation and open to cause reactor trip when the turbine is tripped. No power is provided to the protection system from the contacts: they merely serve to interrupt power to cause reactor trip. This design functions in a deenergize-to-trip fashion to cause a plant trip if power is interrupted in the trip circuitry. This ensures that the protection system will in no way be degraded by this anticipatory trip because seismic

Design considerations do not form part of the design bases for anticipatory trip sensors. (The reactor protection system cabinets which receive the inputs from the anticipatory trip sensors are seismically qualified as discussed in section 3.10.) The anticipatory trips thus meet IEEE Standard 279 including redundancy, separation, single failure, etc. Seismic qualification of the contacts sensors is not required.

The logic for this trip is shown in figure 7.2-1, sheet 16.

7.2.1.1.2.7 Safety Injection Signal Actuation Trip. A reactor trip occurs when a safety injection signal is actuated. The means of actuating a safety injection signal is described in section 7.3.

Figure 7.2-1, sheet 8, shows the logic for this trip.

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

There are no interlocks which can block this trip.
Figure 7.2-1, sheet 3, shows the manual trip logic.

7.2.1.1.3 Reactor Trip System Interlocks

7.2.1.1.3.1 Power Escalation Permissives. The overpower protection provided by the out of core nuclear instrumentation consists of three discrete, but overlapping, ranges. Continuation of startup operation or power increase requires a permissive signal from the higher range instrumentation channels before the lower range level trips can be manually blocked by the operator.

A one-of-two intermediate range permissive signal (P-6) is required prior to source range level trip blocking. A source range manual block is provided for each logic train and the blocks must be in effect on both trains in order to continue power escalation. Source range level trips are automatically reactivated when both intermediate range channels are below the permissive (P-6) level. There are two manual reset switches for administratively reactivating the source range level trip when between the permissive P-6 and P-10 level, if required.
105 Source range level trip block is always maintained when power is above the permissive P-10 level.

Amendment 105
2000. 4.20

The intermediate range level trip and power range (low setpoint) trip can only be blocked after satisfactory operation and permissive information are obtained from two of four power range channels. Individual blocking switches are provided so that the low range power range trip and intermediate range trip can be indenpendently blocked (one switch for each train for a total of four switches). These trips are automatically reactivated when any three of the four power range channels are blow the permissive (P-10) level, thus ensuring automatic activation to more restrictive trip protection.

The development of permissives P-6 and P-10 is shown in figure 7.2-1, sheet 4. All of the permissives are digital: they are derived from analog signals in the nuclear power range and intermediate range channels.

See table 7.2-2 for the list of protection system interlocks.

7.2.1.1.3.2 Blocks of Reactor Trips at Low Power. Interlock P-7 blocks a reactor trip (below approximately 10 percent of full power) on a low reactor coolant flow in more than one loop, reactor coolant pump undervoltage, reactor coolant pump underfrequency, pressurizer low pressure, or pressurizer high water level signal. See figure 7.2-1, sheets 8, 6, and 16, for permissive applications. The low power permissive (P-7) is derived from three out of four power range neutron flux signals below the setpoint in coincidence with two out of two turbine impulse chamber pressure signals below the setpoint (low plant load). The permissive logic is shown in figure 7.2-1, sheets 4 and 16. 31

The P-8 interlock blocks a reactor trip when the plant is below approximately 30 percent of full power on a low reactor coolant flow in any one loop or a turbine trip signal. The block action (absence of the P-8 interlock signal) occurs when three out of four neutron flux power range signals are below the setpoint. Thus, below the P-8 setpoint, the reactor will be allowed to operate with one inactive loop and trip will not occur until two loops are indicating low flow. See figure 7.2-1, sheet 4, for derivation of p-8, and sheet 5 for applicable logic. 31

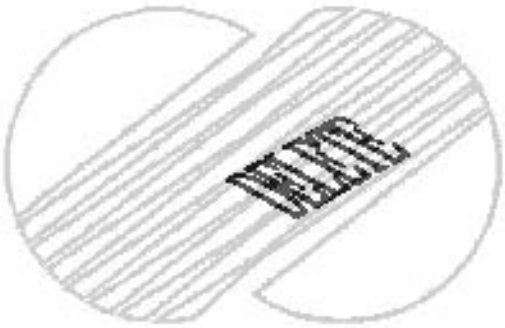
See table 7.2-2 for the list of protection system blocks.

7.2.1.1.4 Coolant Temperature Sensar Arrangement

A. Resistance Temperature Detectcx (RTD).

Hot leg temperature measurement on each toop will be accomplished using three fast response, narrow range, well type dual element RTDs located winthin the thee scoops, which extend into the flow stream at location 120 degrees apart in the cross sectional plane on the reactor coolant hot leg. Cold leg temperature measurement on each loop will be accomplished using one fast response, narrow range, well type dual element RTD located in cold leg at the discharge of the reactor coolant pump. 123

Because of the mixing action of the pump, only one thermowell required to obtain a representative sample. This thermowell is located as close as possible to the weld connection at the pump discharge and is in the same relative position in each loop. 123



123

Signals from these instruments are used to compute the reactor coolant ΔT (temperature of the hot leg, T_{hot}, minus the temperature af the cold leg, T_{cold}) and an average reactor coolant temperature T_{avg}. The T_{avg} for each loop is indicated in the main control room. 123

B. Cold Leg and Hot Leg Temperatures

Temperature detectors, located in the thermometer wells in the cold and hot leg piping of each loop, supply signals to wide range temperature recorders. This information is used by the operator to control coolant temperature during startup and shutdown.

7.2.1.1.5 Pressurizer Water Level Reference Leg Arrangement

The design of the pressurizer water level instrumentation includes a tank level arrangement using differential pressure between an upper and a lower tap.

7.2.1.1.6 Analog System

The analog system consists of two instrumentation systems: the process instrumentation system and the nuclear instrumentation system.

Process instrumentation includes those devices (and their interconnection into systems) which measure temperature, pressure, fluid flow, fluid level as in tanks or vessels, and occasionally physiochemical parameters such as fluid conductivity or chemical concentration. Process instrumentation specifically excludes nuclear and radiation measurements. The process instrumentation includes the process measuring devices, power supplies, indicators, recorders, alarm actuating devices, controllers, signal conditioning devices, etc., which are necessary for day-to-day operation of the nuclear steam supply system, as well as for monitoring the plant and providing initiation of protective functions upon approach to unsafe plant conditions.

The primary function of nuclear instrumentation is to protect the reactor by monitoring the neutron flux and generating appropriate trips and alarms for various phases of reactor operating and shutdown conditions. It also provides a secondary control function and indicates reactor status during startup and power operation. The nuclear instrumentation system uses information from three separate types of instrumentation channels to provide three discrete protection levels. Each range of instrumentation (source, intermediate, and power) provides the necessary overpower reactor trip protection required during operation in that range. The overlap of instrument ranges provides reliable continuous protection beginning with source level through the intermediate and low power level. As the reactor power increases, the overpower protection level is increased by administrative procedures after satisfactory higher range instrumentation operation is obtained. Automatic reset to more restrictive trip protection is provided when reducing power.

Various types of neutron detectors, with appropriate solid-state electronic circuitry, are used to monitor the leakage neutron flux from a completely shutdown condition to 120 percent of full power. The neutron flux covers a wide range between these extremes. Therefore, monitoring with several ranges of instrumentation is necessary.

The lowest range (source range) covers six decades of leakage neutron flux. The lowest observed count rate depends on the strength of the neutron sources in the core and the core multiplication associated with the shutdown reactivity. This is generally greater than two counts per second. The next range (intermediate range) covers eight decades. Detectors and instrumentation are chosen to provide overlap between the higher portion of the source range and the lower portion of the intermediate range. The highest range of instrumentation (power range) covers approximately two decades of the total instrumentation range. This is a linear range that overlaps with the higher portion of the intermediate range.

The system described above provides control room indication and recording of signals proportional to reactor neutron flux during core loading, shutdown, startup, and power operation, as well as during subsequent refueling. Startup rate indication for the source and intermediate range channels is provided in the control room. Reactor trip, rod stop, control and alarm signals are transmitted to the reactor control and protection system for automatic plant control. Equipment failures and test status information are annunciated in the control room.

See references 1 and 2 for additional background information on the process and nuclear instrumentation.

7.2.1.1.7 Solid-State Protection System

The solid-state logic protection system takes binary inputs (voltage/no voltage) from the process and nuclear instrument channels corresponding to conditions (normal/abnormal) of plant parameters. The system combines these signals in the required logic combination and generates a trip signal (no voltage) to the undervoltage trip attachment and the shunt trip auxiliary coils of the reactor trip circuit breakers when the necessary combination of signals occurs. The system also provides annunciator, status light, and computer input signals which indicate the condition of bistable input signals, partial trip and full trip functions, and the status of the various blocking, permissive and actuation functions. In addition, the system includes means for semiautomatic testing of the logic circuits. A detailed description of this system is given in reference 3.

7.2.1.1.8 Isolation Amplifiers

In certain applications, it is advantageous to employ control signals derived from individual protection channels through isolation amplifiers contained in the protection channel, as permitted by IEEE Standard 279.

In all of these cases, analog signals derived from protection channels for nonprotective functions are obtained through isolation amplifiers located in the analog protection racks. By definition, nonprotective functions include those signals used for control, remote process indication, and computer monitoring. Isolation amplifier qualification type tests are described in references 6 and 7 and additional Westinghouse test programs are discussed in section 7.1.

7.2.1.1.9 Energy Supply and Environmental Variations

The energy supply for the reactor trip system, including the voltage and frequency variations, is described in section 7.6 and chapter 8. The environmental variations, throughout which the system will perform, are given in section 3.11 and chapter 8.

7.2.1.1.10 Setpoints

The setpoints that require trip action are given in ITS Chapter 1. A further discussion on setpoints is found in subparagraph 7.1.2.1.9. | 845

7.2.1.1.11 Seismic Design

The seismic design considerations for the reactor trip system are given in section 3.10. This design meets the requirements of General Design Criterion 2.

7.2.1.2 Design Bases Information

The information given below presents the design bases information requested by Section 3 of IEEE Standard 279 Functional logic diagrams are presented in figure 7.2-1.

7.2.1.2.1 Generating Station Conditions

The following are the generating station conditions requiring reactor trip:

479 A. DNBR approaching limit value

B. Power density (kW/ft) approaching rated value for Condition II faults (see chapter 4 for fuel design limits)

C. Reactor coolant system overpressure creating stresses approaching the limits specified in chapter 5,

7.2.1.2.2 Generating Station Variables

The following are the variables required to be automatically monitored in order to provide reactor trips (see table 7.2-1).

A. Neutron flux

B. Reactor coolant temperature

C. Reactor coolant system pressure (pressurizer pressure)

D. Pressurizer water level

E. Reactor coolant flow

F. Reactor coolant pump operational status (voltage and frequency)

G. Steam generator water level

H. Turbine generator operational status (trip fluid pressure and stop valve position).

7.2.1.2.3 Spatially Dependent Variables

Reactor coolant temperature is spatially dependent.

See paragraph 7.3.1.2 for a discussion of this variable spatial dependence.

7.2.1.2.4 Limits and Margins

The parameter values that will require reactor trip are given in ITS, Technical Specifications, and in chapter 15, Accident Analyses. Chapter 15 demonstrates that the setpoints used in ITS Chapter 1 are conservative. 343 343

The setpoints for the various functions in the reactor trip system have been analytically determined such that the operational limits so prescribed will prevent fuel rod clad damage and loss of integrity of the reactor coolant system (RCS) as a result of any ANS Condition II incident (anticipated malfunction). As such, during any ANS Condition II incident, the reactor trip system limits the following parameters to:

Minimum DNBR = limit value 479

Maximum system pressure = 2750 psia

Fuel rod maximum linear power =22.5 kW/ft 479

The accident analyses described in chapter 15 demonstrate that the functional requirements as specified for the reactor trip system are adequate to meet the above considerations, even assuming, for conservatism, adverse combinations of instrument errors (refer to table 7.2-3). A discussion of the safety limits associated with the reactor core and RCS, plus the limiting safety system setpoints, is presented in the technical specifications.

7.2.1.2.5 Abnormal Events

The following malfunctions, accidents, or other unusual events which could physically damage reactor trip system components or could cause environmental changes are considered in design:

A. Earthquakes (see chapters 2 and 3)

B. Fire (see section 9.5)

C. Explosion (hydrogen buildup inside containment, see subsection 6.2.5)

D. Missiles (see section 3.5)

E. Flood (see chapters 2 and 3)

F. Wind and tornadoes (see section 3.3).

The reactor trip system fulfills the requirements of IEEE Standard 279 to provide automatic protection and to provide initiating signals to mitigate the consequences of faulted conditions. The reactor trip system relies upon provisions made by the owner and operator of the plant to provide protection against destruction of the system from fires, explosions, floods, wind, and tornadoes (see each item above). The discussions in subparagraph 7.1.2.1.7 and this section adequately address or reference the coverage of the affects of abnormal events on the reactor trip system in conformance with applicable General Design Criteria.

7.2.1.2.6 Minimum Performance Requirements

7.2.1.2.6.1 Reactor Trip System Response Times. Reactor trip system response time is defined in section 7.1. Typical maximum allowable time delays in generating the reactor trip signal are tabulated in table 7.2-3. Reactor trip system instrumentation
343 response times are provided in ITS Chapter 1 table 3.3.1-2. During preliminary startup tests, it will be demonstrated that actual time delays of installed equipment are equal to or less than the values assumed in the accident analyses. (See paragraph 7.1.2.28 for a discussion of periodic response time verification capabilities.)

7.2.1.2.6.2 Reactor Trip Accuracies. Accuracy is defined in
479 section 7.1. Accuracies are tabulated in table 7.2-3. The trip setpoint is determined by factors other than the most accurate portion of the instrument's range. The safety limit setpoint is determined only by the accident analysis. As described above, allowance is then made for process uncertainties, instrument error, instrument drift, and calibration uncertainty to obtain the nominal setpoint value which is actually set into the equipment. The only requirement on the instrument's accuracy value is that over the instrument span, the error must always be less than or equal to the error value allowed in the accident analysis. The instrument does not need to be the most accurate at the setpoint value as long as it meets the minimum accuracy requirement. The accident analysis accounts for the expected errors at the actual setpoint.

7.2.1.2.6.3 Protection System Ranges. Typical protection system ranges are tabulated in table 7.2-3. Range selection for the instrumentation covers the expected range of the process variable being monitored during power operation. Limiting setpoints are at least 5 percent from the end of the instrument span.

7.2.1.3 Final Systems Drawings

Final electrical schematic drawings, logics, piping and instrumentation diagrams and location drawings are provided in the final systems drawing package. Any significant functional differences between the PSAR and FSAR are accommodated in the drawings listed in table 1.7-1.

7.2.2 ANALYSIS

7.2.2.1 Failure Mode and Effects Analysis

A failure mode and effects analysis of the reactor trip system has been performed. Results of this fault tree analysis are presented in reference 4.

7.2.2.2 Evaluation of Design Limits

While most setpoints used in the reactor protection system are fixed, there are variable setpoints, most notably the over-temperature ΔT and overpower ΔT setpoints. All setpoints in the reactor trip system have been selected on the basis of engineering design or safety studies. The capability of the reactor trip system to prevent loss of integrity of the fuel clad and/or RCS pressure boundary during Condition II and III transients is demonstrated in chapter 15. These accident analyses are carried out using those setpoints determined from results of the engineering design studies. Setpoint limits are presented in the technical specifications. A discussion of the intent for each of the various reactor trips and the accident analyses (where appropriate) which utilize this trip is presented below. It should be noted that the selected trip setpoints all provide for margin before protection action is actually required to allow for uncertainties and instrument errors. The design meets the requirements for General Design Criteria 10 and 20.

7.2.2..2.1 Trip Setpoint Discussion

It has been pointed out previously that below a DNBR of 1.30 there is likely to be significant local fuel clad failure. The DNBR existing at any point in the core for a given core design can be determined as a function of the core inlet temperature, power output, operating pressure, and flow. Consequently, core safety limits in terms of a DNBR equal to 1.30 for the hot channel can be developed as a function of core ΔT, T_{avg} and pressure for a specified flow as illustrated by the solid lines in figure 7.2-3. Also shown as solid lines in figure 7.2-3 are the logic of conditions equivalent to 118 percent of power as a function of ΔT and T_{avg} representing the overpower (kW/ft)

limit on the fuel. The dashed lines indicate the maximum permissible setpoint (ΔT) as a function of T_{avg} and pressure for the over-temperature and overpower reactor trip. Actual values of setpoint constants in the equation representing the dashed lines are as given in the technical specifications. These values are conservative to allow for instrument errors. The design meets the requirements of General Design Criteria 10, 15, 20, and 29.

DNBR is not a directly measurable quantity; however, the process variables that determine DNBR are sensed and evaluated. Small isolated changes in various process variables may not individually result in violation of a core safety limit; whereas, the combined variations, over sufficient time, may cause the overpower or overtemperature safety limit to be exceeded. The design concept of the reactor trip system accommodates this situation by providing reactor trips associated with individual process variables in addition to the overpower/overtemperature safety limit trips. Process variable trips prevent reactor operation whenever a change in the monitored value is such that a core or system safety limit is in danger of being exceeded should operation continue. Basically, the high pressure, low pressure, and overpower/overtemperature ΔT trips provide sufficient protection for slow transients as opposed to such trips as low flow or high flux which will trip the reactor rapidly for changes in flow or flux, respectively, that would result in fuel damage before actuation of the slower responding ΔT trips could be effected.

Therefore, the reactor trip system has been designed to provide protection for fuel cladding and RCS pressure boundary integrity where: 1) a rapid change in a single variable or factor will result in exceeding a core or a system safety limit, and 2) a slow change in one or more variables will have an integrated effect which will cause safety limits to be exceeded. Overall, the reactor trip system offers diverse and comprehensive protection against fuel clad failure and/or loss of RCS integrity for Condition II and III accidents. This is demonstrated by table 7.2-4 which lists the various trips of the reactor trip system, the corresponding technical specification on safety limits and safety system settings, and the appropriate accident discussed in the safety analyses in which the trip could be utilized.

The reactor trip system design was evaluated in detail with respect to common mode failure and is presented in references 4 and 5. The design meets the requirements of General Design Criterion 21.

Preoperational testing is performed on reactor trip system components and systems to determine equipment readiness for startup. This testing serves as a further evaluation of the system design.

Analyses of the results of Condition I, II, III, and IV events, including considerations of instrumentation installed to mitigate their consequences, are presented in chapter 15. The instrumentation installed to mitigate the consequences of load rejection and turbine trip is given in section 7.4.

7.2.2.2.2 Reactor Coolant Flow Measurement

The elbow taps used on each loop in the RCS are instrument devices that indicate the status of the reactor coolant flow. The basic function of these devices is to provide information as to whether or not a reduction in flow has occurred. The correlation between flow and elbow tap signal is given by the following equation:

$$\frac{\Delta P}{\Delta P_o} = \left(\frac{w}{w_o}\right)^2$$

where ΔP_o is the pressure differential at the reference flow w_o, and ΔP is the pressure differential at the corresponding flow, w. The full flow reference point is established during initial plant startup. The low flow trip point is then established by extrapolating along the correlation curve. The expected accuracy of the channel is within ±10 percent of full flow and field results have shown the repeatability of the trip point to be within ±1 percent.

7.2.2.2.3 Evaluation of Compliance to Applicable Codes and Standards

The reactor trip system meets the criteria of the General Design Criteria and the criteria of IEEE Standard 279 as indicated below.

7.2.2.2.3.1 General Functional Requirement. The protection system automatically initiates appropriate protective action whenever a condition monitored by the system reaches a preset level. Functional performance requirements are given in subparagraph 7.2.1.1.1. Subparagraph 7.2.1.2.4 presents a discussion of limits and margins; subparagraph 7.2.1.2.5 discusses unusual (abnormal) events; and subparagraph 7.2.1.2.6 presents minimum performance requirements.

7.2.2.2.3.2 Single Failure Criterion. The protection system is designed to provide two, three, or four instrumentation channels for each protective function and two logic train circuits. These redundant channels and trains are electrically isolated and physically separated. Thus, any single failure within a channel or train will not prevent protective action at the system level when required. Loss of input power, the most likely mode of failure, to a channel or logic train will result in a signal calling for a trip. This design meets the requirements of General Design Criterion 23.

To prevent the occurrence of common mode failures, such additional measures as functional diversity, physical separation, and testing as well as administrative control during design, production, installation, testing, and operation are employed, as discussed in reference 4. The design meets the requirements of General Design Criteria 21 and 22.

7.2.2.2.3.3 Quality of Components and Modules. For a discussion of the quality of the components and modules used in the reactor trip system, refer to a separately published QA manual. The quality assurance applied conforms to General Design Criterion 1.

51

7.2.2.2.3.4 Equipment Qualification. For a discussion of the type tests made to verify the performance requirements, refer to sections 3.10 and 3.11. The test results demonstrate that the design meets the requirements of General Design Criterion 4.

7.2.2.2.3.5 Channel Integrity. Protection system channels required to operate in accident conditions maintain necessary functional capability under extremes of conditions relating to environment, energy supply, malfunctions, and accidents. The energy supply for the reactor trip system is described in section 7.6 and chapter 8. The environmental variations throughout which the system will perform are given in section 3.11.

7.2.2.2.3.6. Independence. Channel independence is carried throughout the system, extending from the sensor through the devices actuating the protective function. Physical separation is used to achieve separation of redundant transmitters. Separation of wiring is achieved using separate wire ways, cable trays, conduit runs, and containment penetrations for each redundant channel. Redundant analog equipment is separated by locating modules in different protection cabinets. Each redundant protection channel set is energized from a separate ac power feed. This design meets the requirements of General Design Criterion 21.

Independence of the logic train is discussed in reference 3. Two reactor trip breakers are actuated by two separate logic matrices which interrupt power to the control rod drive mechanisms.

The breaker main contacts are connected in series with the power supply so that opening either breaker interrupts power to all full length control rod drive mechanisms, permitting the rods to free fall into the core (see figure 7.2-4).

The design philosophy is to make maximum use of a wide variety of measurements. The protection system continuously monitors numerous diverse system variables. The extent of this diversity has been evaluated for a wide variety of postulated accidents and is discussed in reference 5. Generally, two or more diverse protection functions would terminate an accident before intolerable consequences could occur. This design meets the requirements of General Design Criterion 22.

7.2.2.2.3.7 Control and Protection System Interaction. The protection system is designed to be independent of the control system. In certain applications, the control signals and other nonprotective functions are derived from individual protective channels through isolation amplifiers. The isolation amplifiers are classified as part of the protection system and are located in the analog protective racks. Nonprotective functions include those signals used for control, remote process indication, and computer monitoring. The isolation amplifiers are designed such that a short circuit, open circuit, or the application of 118V ac or 140V dc on the isolated output portion of the circuit (i.e., the nonprotective side of the circuit) will not affect the input (protective) side of the circuit. The signals obtained through the isolation amplifiers are never returned to the protective racks. This design meets the requirements of General Design Criterion 24 and Section 4.7 of IEEE Standard 279.

A detailed discussion of the design and testing of the isolation amplifiers is given in references 6 and 7. These reports include the results of applying various malfunction conditions on the output portion of the isolation amplifiers. The results show that no significant disturbance to the isolation amplifier input signal occurred.

7.2.2.2.3.8 Derivation of System Inputs. To the extent feasible and practical, protection system inputs are derived from signals which are direct measures of the desired variables. Variables monitored for the various reactor trips are listed in subparagraph 7.2.1.2.2.

7.2.2.2.3.9 Capability for Sensor Checks. The operational availability of each system input sensor during reactor operation is accomplished by cross checking between channels that bear a known relationship to each other and that have
646 readouts available. Channel checks are discussed in ITS Chapter 1.

7.2.2.2.3.10 Capability for Testing. The reactor trip system is capable of being tested during power operation. Where only parts of the system are tested at any one time, the testing sequence provides the necessary overlap between the parts to assure complete system operation. The testing capabilities are in agreement with Regulatory Guide 1.22 as discussed in paragraph 7.1.2.5.

The protection system is designed to permit periodic testing of the analog channel portion of the reactor trip system during reactor power operation without initiating a protective action unless a trip condition actually exists. This is because of the coincidence logic required for reactor trip. These tests may be performed at any plant power from cold shutdown to full power. Before starting any of these tests with the plant at power, all redundant reactor trip channels associated with the function to be tested must be in the normal (untripped) mode in order to avoid spurious trips. Setpoints are referenced in the precautions, limitation, and setpoints portion of the plant technical manual.

A. Analog Channel Tests

Analog channel testing is performed at the analog instrumentation cabinet by individually introducing dummy input signals into the instrumentation channels and observing the tripping of the appropriate output bistables. Briefly, in the analog racks, lamps and analog test switches are provided. The bistable output is put in a trip condition by placing the test switch in the test position. This action connects the proving lamp to the bistable and disconnects and thus de-energizes (operates) the bistable output relays in train A and train B logic cabinets and allows injection of a test signal to the channel. Relay logic in the process cabinets automatically blocks the test signal unless the bistable amplifier is tripped. This, of necessity, is done on one channel at a time. Interruption of the bistable output to the logic circuitry for any cause test, maintenance purposes, or removed from service) will cause that portion of the logic to be actuated (partial trip) accompanied by a partial trip alarm and channel status light actuation in the control room. A signal is then inserted through a test jack. Verification of the bistable trip setting is now

confirmed by the Proving lamp. Each channel contains those switches, test points, etc., necessary to test the channel. It is estimated that analog testing can be performed at a rate of several channels per hour. See reference 1 for additional information.

The following periodic tests of the analog channels of the protection circuits are performed:

T_{avg} and ΔT protection channel testing

Pressurizer pressure protection channel testing

Pressurizer water level protection channel testing

Steam generator water level protection channel testing

Reactor coolant low flow, underfrequency, and undervoltage protection channels.

Turbine impulse chamber pressure channel testing

Steam pressure protection channel testing

Containment pressure channel testing.

B. Nuclear Instrumentation Channel Tests

The power range channels of the nuclear instrumentation system are tested by superimposing a test signal on the actual detector signal being received by the channel at the time of testing. The output of the bistable is not placed in a tripped condition prior to testing. Also, since the power range channel logic is two out of four, bypass of this reactor trip function is not required.

To test a power range channel, a "TEST-OPERATE" switch is provided to require deliberate operator action, the operation of which will initiate the "CHANNEL TEST" annunciator in the control room. Bistable operation is tested by increasing the test signal level to bistable trip setpoint and verifying bistable relay operation by control board annunciation and trip status lights.

It should be noted that a valid trip signal would cause the channel under test to trip at a lower actual reactor power level. A reactor trip would occur when a second bistable trips. No provision has been made in the channel test circuit for reducing the channel signal level below that signal being received from the nuclear instrumentation system detector.

A nuclear instrumentation system channel which can cause a reactor trip through one of two protection logic (source or intermediate range) is provided with a bypass function which prevents the initiation of a reactor trip from that particular channel during the short period that it is undergoing test. These bypasses are annunciated in the control room.

The following periodic tests of the nuclear instrumentation system are performed :

1. Testing at plant shutdown

   Source range testing
   Intermediate range testing
   Power range testing

2. Testing between P-6 and P-10 permissive power levels

   Source range testing
   Intermediate range testing

3. Testing above P-10 permissive power level

   Power range testing

Any deviations noted during the performance of these tests are investigated and corrected in accordance with the established calibration and troubleshooting procedures provided in the plant technical manual for the nuclear instrumentation system. Control and protection trip settings are indicated in the plant technical manual under precautions, limitations, and setpoints.

For additional background information on the nuclear instrumentation system, see reference 2.

C. Solid-State Logic Testing

The reactor logic trains of the reactor trip system are designed to be capable of complete testing at power. After the individual channel analog testing is complete, the logic matrices are tested from the train A and train B logic rack test panels. This step provides overlap between the analog and logic portions of the test program. During this test, each of the logic inputs is actuated automatically in all combinations of trip and non-trip logic. Trip logic is not maintained long enough to permit master relay actuation (master relays are pulsed in order to check continuity). Following the logic testing, the individual master relays are actuated electrically to

test their mechanical operation. Actuation of the master relays during this test will apply low voltage to the slave relay coil circuits to allow continuity checking, but not slave relay actuation. During logic testing of one train, the other train can initiate any required protective functions. Annunciation is provided in the control room to indicate when a train is in test (train output bypassed) and when a reactor trip breaker is bypassed. Logic testing can be performed in less than 30 minutes. Details of the logic system testing are given in reference 3.

A direct reactor trip resulting from undervoltage or underfrequency on the reactor coolant pump buses is provided as discussed in subsection 7.2.1 and as shown in figure 7.2-1. The logic for these trips is capable of being tested during power operation. When parts of the trip are being tested, the sequence is such that an overlap is provided between parts so that a complete logic test is provided. Opening of the reactor coolant pump breakers during power operation is not possible since a reactor trip would occur as a result of low reactor coolant flow.

This design complies with the testing requirements of the applicable criteria as addressed in paragraph 7.1.2.5. Details of the method of testing and compliance with these standards are provided in subparagraph 7.2.2.2.3.

The permissive and block interlocks associated with the reactor trip system and ESF are given in tables 7.2-2 and 7.3-3 and designated protection or "P" interlocks. As a part of the protection system, these interlocks are designed to meet the testing requirements of IEEE Standards 279 and 338.

Testing of all protection system interlocks is provided by the logic testing and semi-automatic testing capabilities of the solidstate protection system. In the solid-state protection system, the undervoltage coils (reactor trip) and master relays (engineered safeguards actuation) are pulsed for all combinations of trip or actuation logic with and without the interlock signals. For example, reactor trip on low flow is tested to verify operability of the trip above P-7 and non-trip below P-7. (See figure 7.2-1, sheet 5.) Interlock testing may be performed at power.

Testing of the logic trains of the reactor trip system includes a check of the input relays and a logic matrix check. The following sequence is used to test the system:

1. Check of input relays

   During testing of the process instrumentation system and nuclear instrumentation system channels, each channel bistable is placed in a trip mode causing one input relay in train A and one in train B to de-energize. A contact of each relay is connected to a universal logic printed circuit card. This card performs both the reactor trip and monitoring functions. Each reactor trip input relay contact causes a status lamp and an annunciator on the control board to operate. Either the train A or train B input relay operation will light the status lamp and annunciator.

   Each train contains a multiplexing test switch. At the start of a process or nuclear instrumentation system test, this switch (in either train) is placed in the A + B position. The A + B position alternately allows information to be transmitted from the two trains to the control board. A steady status lamp and annunciator indicates that input relays in both trains have been de-energized. A flashing lamp means that the input relays in the two trains did not both de-energize. Contact inputs to the logic protection system such as reactor coolant pump bus underfrequency relays operate input relays which are tested by operating the remote contacts as described above and using the same type of indications as those provided for bistable input relays.

   Actuation of the input relays provides the overlap between the testing of the logic protection system and the testing of those systems supplying the inputs to the logic protection system. Test indications are status lamps and annunciators on the control board. Inputs to the logic protection system are checked one channel at a time, leaving the other channels in service. For example, a function that trips the reactor when two out of four channels trip becomes a one-out-of-three trip when one channel is placed in the trip mode. Both trains of the logic protection system remain in service during this portion of the test.

2. Check of logic matrices

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

The logic test scheme uses pulse techniques to check the coincidence logic. All possible trip and non-trip combinations are checked. Pulses from the tester are applied to the inputs of the universal logic card at the same terminals that connect to the input relay contacts. Thus, there is an overlap between the input relay check and the logic matrix check. Pulses are fed back from the reactor trip breaker undervoltage trip attachment and the shunt trip auxiliary relay coils to the tester. The pulses are of such short duration that neither the reactor trip breaker undervoltage attachment nor the shunt trip auxiliary relay can respond mechanically. 3

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

The general design features and details of the testability of the logic system are described in reference 3. The testing capability meets the requirements of General Design Criterion 21.

D. Testing of Reactor Trip Breakers

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

1. With bypass breaker 52/BYA racked out, manually close and trip it to verify its operation.

3

2. Rack in and close 52/BYA. Manually trip 52/RTA through a protection system logic matrix while at the same time depressing the "auto shunt trip block" push button on the automatic shunt trip pannel. This verifies operation of the undervoltage trip attachment. When the breaker trip. After reclosing 52 BTA. trip it again by depressing the "Auto shunt trip test" push botton on the automatic shunt trip panel. This verifies tripping of the breaker through the shunt trip device.

3. Reset 52/RTA.

4. Trip and rack out 52/BYA.

5. Repeat above steps to test trip breaker 52/RTB using bypass breaker 52/BYB.

Auxiliary contacts of the bypass breakers are connected into the alarm system of their respective trains such that if either train is placed in test while the bypass breaker of the other train is closed, both reactor trip breakers and both bypass breakers will automatically trip.

Auxiliary contacts of the bypass breakers are also connected in such a way that if an attempt is made to close the bypass breaker in one train while the bypass breaker of the other train is already closed, both bypass breakers will automatically trip.

The train A and train B alarm systems operate separate annunciators in the control room. The two bypass breakers also operate an annunciator in the control room. Bypassing of a protection train with either the bypass breaker or with the test switches will result in audible and visual indications.

The complete reactor trip system is normally required to be in service. However, to permit online testing of the various protection channels or to permit continued operation in the event of a subsystem instrumentation channel failure, a technical specification defining the minimum number of operable channels and the minimum degree of channel redundancy has been formulated. This technical specification also defines the required restriction to operation in the event that the channel operability and degree of redundancy requirements cannot be met.

7.2.2.2.3.11 Channel Bypass or Removal from Operation. The protection system is designed to permit periodic testing of the analog channel portion of the reactor trip system during reactor power operation without initiating a protective action unless a trip condition actually exists. This is because of the coincidence logic required for reactor trip.

7.2.2.2.3.12 Bypasses. Where normal operating requirements necessitate automatic or manual bypass of a protective function, the design is such that the bypass is removed automatically whenever permissive conditions are not met. Devices used to achieve automatic removal of the bypass of a protective function are considered part of the protective system and are designed in accordance with the criteria of this section. Indication is provided in the control room if some part of the system has been administratively bypassed or taken out of service.

7.2.2.2.3.13 Indication of Bypasses. Bypass indication is discussed in paragraph 7.1.2.10.

7.2.2.2.3.14 Access to Means for Bypassing. The design provides for administrative control of access to the means for manually bypassing channels or protective functions. For additional background information, refer to reference 1.

7.2.2.2.3.15 Multiple Setpoints. For monitoring neutron flux, multiple setpoints are used. When a more restrictive trip setting becomes necessary to provide adequate protection for a particular mode of operation or set of operating conditions, the protective system circuits are designed to provide positive means or administrative control to assure that the more restrictive trip setpoint is used. The devices used to prevent improper use of less restrictive trip settings are considered part of the protective system and are designed in accordance with the criteria of this section.

7.2.2.2.3.16 Completion of Protective Action. The protection system is so designed that, once initiated, a protective action goes to completion. Return to normal operation requires action by the operator.

7.2.2.2.3.17 Manual Initiation. Switches are provided on the control board for manual initiation of protective action. Failure in the automatic system does not prevent the manual actuation of the protective functions. Manual actuation relies on the operation of a minimum of equipment.

7.2.2.2.3.18 Access. The design provides for administrative control of access to all setpoint adjustments, module calibration adjustments, test points, and the means for manually bypassing channels or protective functions. For additional background information, refer to reference 1.

7.2.2.2.3.19 Identification of Protective Actions. Protective channel identification is discussed in paragraph 7.1.2.3. Indication is discussed in the following section.

7.2.2.2.3.20 Information Readout. The protective system provides the operator with complete information pertinent to system status and safety. All transmitted signals (flow, pressure, temperature, etc.) which can cause a reactor trip will be either indicated or recorded for every channel, including all neutron flux power range currents (top detector, bottom detector, algebraic difference and average of bottom and top detector currents).

Any reactor trip will actuate an alarm and an annunciator. Such protective actions are indicated and identified down to the channel level.

Annunciators are also used to alert the operator to deviations from normal operating conditions so that he may take appropriate corrective action to avoid a reactor trip. For example, actuation of any rod stop or trip of any channel will actuate a visual and audible alarm.

7.2.2.2.3.21 System Repair. The protection system is designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.

7.2.2.3 Specific Control and Protection Interaction

7.2.2.3.1 Neutron Flux

The flux differences between the upper and lower ion chambers from three of the four power range, neutron channels are used as inputs to the overtemperature ΔT and overpower ΔT setpoints. The isolated nuclear power signal from the fourth channel is used for automatic rod control.

In addition, channel deviation signals in the control system will give an alarm if any power range channel deviation occurs. Also, the control system will respond only to rapid changes in indicated neutron flux: slow changes or drifts are compensated by the temperature control signals. Finally, an overpower signal from any nuclear power range channel will block manual and automatic rod withdrawal. The setpoint for this rod stop is below the reactor trip setpoint.

7.2.2.3.2 Coolant Temperature

The accuracy of the resistance temperature detector (RTD) temperature measurements is demonstrated during plant start-up tests by comparing temperature measurements from all loop RTDS with one another as well as with the temperature measurements obtained from the RTD located in the hot leg and cold leg piping of each loop. 123

The linearity of the △T measurements obtained from the hot leg and cold leg RTDs as a function of power is also checked during plant startup tests. The absolute value of ΔT versus power is not important, per se, as far as reactor protection is concerned, Reactor trip system setpoints are based upon percentages of the indicated △T. This is dune to account for inherent loop differences. The percent ΔT input is a relative, not absolute input for reactor trip, and therefore, provides better protective action. For this reason, the linearity of the △T signals as a function of power is more significant than the absolute values of the ΔT. As part of the plant startup tests, the RTD signals will be compared with the core exit thermocouple signals.

Since control is based on the temperature of the loop with the median average temperature, control rod movement is based upon the median temperature measurement with respect to margins to DNB. A spurious low and high average temperature measurement from any loop temperature control channel will not affect control action, 123

DELETE

In addition, channel deviation signals in the control system will give an alarm if any temperature channel deviates significantly from the auctioneered (highest) value. Automatic rod withdrawal blocks and turbine runback (power demand reduction) will also occur if any two of the four overtemperature or overpower △T channels indicate an adverse condition.

7.2.2.3.3 Pressurizer Pressure

The pressurizer pressure protection channel signals are used for high and low pressure protection and as inputs to the overtemperature △T trip protection function. Control channels (separate from the protection channels) generate signals which
460 are used to control pressurizer spray and heaters. Delete

A spurious high pressure signal from one channel can cause decreasing pressure by actuation of either spray or relief valves. Additional redundancy is provided in the low pressurizer pressure reactor trip logic and in the logic for safety injection to ensure low pressure protection.

Overpressure protection is based upon the maximum positive surge of the reactor coolant produced as a result of turbine trip under full load, assuming the core continues to produce full power with normal feed flow maintained. The self-actuated safety valves are sized on the basis of steam flow from the pressurizer to accommodate this surge at a setpoint of 2500 psia and an accumulation of 3 percent. Note that no credit is taken for the relief capability provided by the power-operated relief valves during this surge, or the turbine bypass system. In addition, operation of any one of the power-operated relief valves can maintain pressure below the high pressure trip point for most transients.

The pressurizer heaters will not overpressurize the RCS because the rate of pressure rise achievable with heaters is slow, and ample time and pressure alarms are available to alert the opbrator to the need for appropriate action.

7.2.2.3.4 Pressurizer Water Level

Three pressurizer water level channels are used for high pressurizer water level reactor trip. Isolated signals from these channels are used for pressurizer water level control. A failure in the level control system could fill or empty the pressurizer at a slow rate (on the order of half an hour or more), which allows ample time for corrective action.

Amendment 460
2010.3.5

The high water level trip setpoint provides sufficient margin such that discharging liquid coolant through the safety valves is avoided. Even at full power conditions, which would produce the worst thermal expansion rates, a failure of the water level control would not lead to any liquid discharge through the safety valves. This is due to the automatic high pressurizer pressure reactor trip actuating at a pressure sufficiently below the safety valve setpoint, or to the high pressurizer water level reactor trip.

7.2.2.3.5 Steam Generator Water Level

The reactor protection circuits associated with low-low steam generator water level ensure that the steam generator heat sink is available for removal of long-term residual heat. Should a complete loss of feedwater occur, the reactor would be tripped on low-low steam generator water level. In addition, redundant auxiliary feedwater pumps are provided to supply feedwater in order to remove residual heat after trip. This reactor trip acts before the steam generators are dry to reduce the required capacity and starting time requirements of these auxiliary feedwater pumps and to minimize the thermal transient on the RCS and steam generators.

Two-out-of-four low-low steam generator water level trip logic ensures a reactor trip, if needed, even with an independent failure in another channel used for control and when degraded by an additional second postulated random failure.

A spurious high signal from the feedwater flow channel being used for control would cause a reduction in feedwater flow. However, the mismatch between steam demand and feedwater flow produced by this spurious signal will actuate alarms to alert the operator to this situation in time for manual correction, or, if the condition continues, the reactor will trip on a low-low water level signal independent of indicated feedwater flow.

A spurious low signal from the feedwater flow channel being used for control would cause an increase in feedwater flow. The mismatch between steam flow and feedwater flow produced by the spurious signal would actuate alarms to alert the operator to the situation in time for manual correction. If the condition continues, a two-out-of-three high-high steam generator water level signal in any loop, independent of the indicated feedwater flow, will cause feedwater pump trip and isolation and trip the turbine. The turbine trip will result in a subsequent reactor trip if power is above the P-8 setpoint. The high-high steam generator water level trip is an equipment protective trip preventing excessive moisture carryover which could damage the turbine blading. |3

In addition, the three element feedwater controller incorporates reset action on the level error signal, such that with expected controller settings a rapid increase or decrease in the flow signal would cause only a small change in level before the controller would compensate for the level error. A slow change in the feedwater signal would have no effect at all. A spurious low or high steam flow signal would have the same effect as high or low feedwater flow signal, discussed above.

A spurious high steam generator water level signal from the protection channel used for control will tend to close the feedwater valve. However, before a reactor trip would occur, two out of three channels for a steam generator would have to indicate a high water level. A spurious low steam generator water level signal will tend to open the feedwater valve. Again, before a reactor trip would occur, two out of four channels in a loop would have to indicate a low water level. Any slow drift in the water level signal will permit the operator to respond to the level alarms and take corrective action. Automatic protection is provided in case the spurious high level reduces feedwater flow sufficiently to cause low level in the steam generator. Automatic protection is provided in case the spurious low level signal increases feedwater flow sufficiently to cause high level in the steam generator. A turbine trip and feedwater isolation would occur in two out of three high-high steam generator water levels in any loop.

7.2.2.4 Additional Postulated Accidents

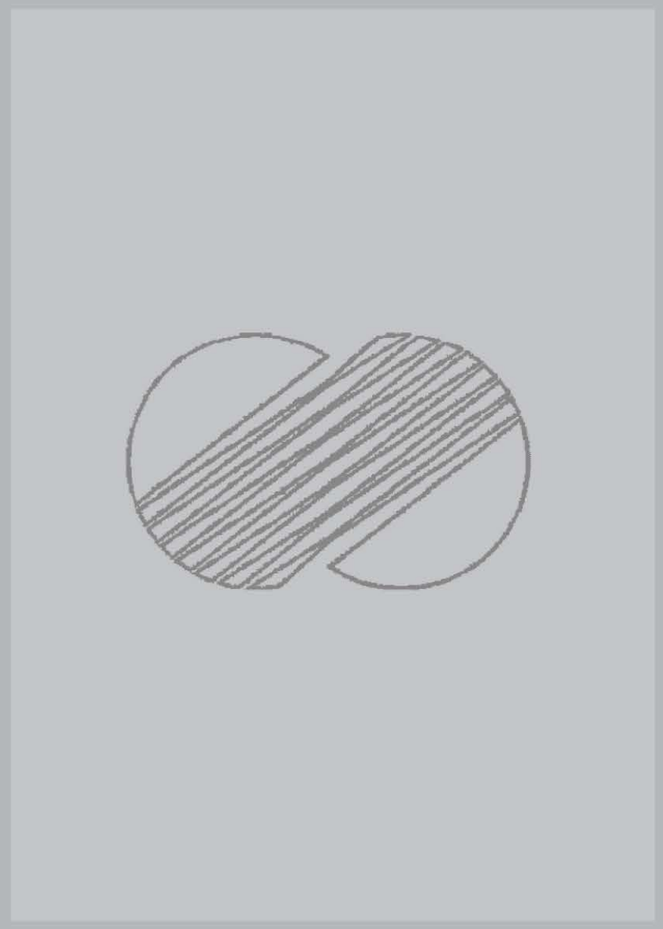
Loss of plant instrument air or loss of reactor plant component cooling water is discussed in paragraph 7.3.3.1. Load rejection and turbine trip are discussed in further detail in section 7.7.

The control interlocks, called rod stops, that are provided to prevent abnormal power conditions which could result from excessive control rod withdrawal, are discussed in subparagraph 7.7.1.4.1 and are listed in table 7.7-1. Excessively high power operation (which is prevented by locking of automatic rod withdrawal), if allowed to continue, might lead to a safety
849 limit (as given in ITS Chapter 1) being reached. Before such a limit is reached, protection will be available from the reactor trip system. At the power levels of the rod block setpoints, safety limits have not been reached: therefore, these rod withdrawal stops do not come under the scope of safety-related systems, and are considered as control systems.

374
2.05

Korea Hydro & Nuclear Power Company
YGN 1 & 2 FSAR

INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(SHEET 1 OF 18)
Figure 7.2-1

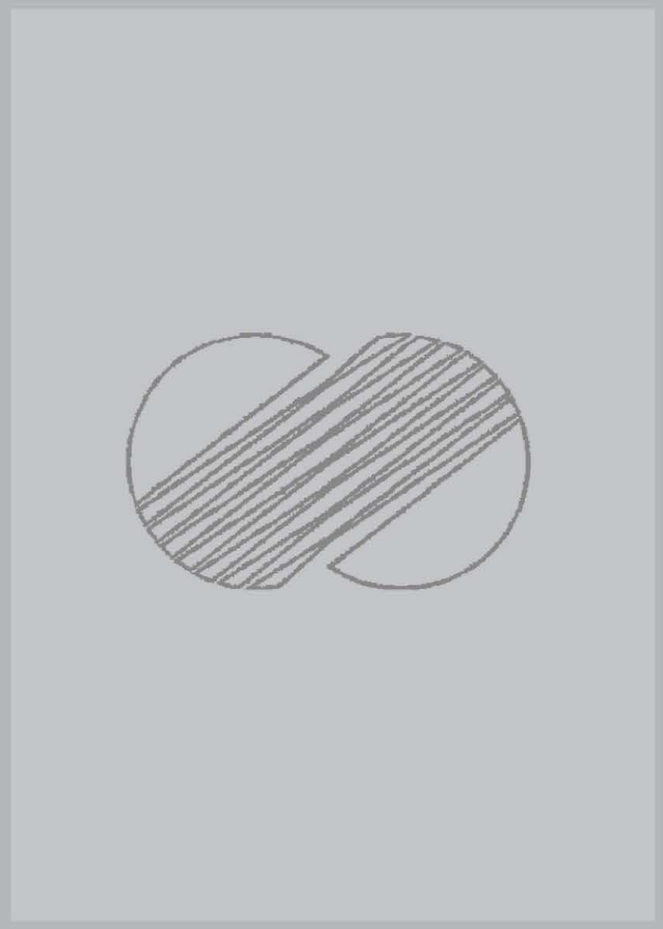


Amendment 31
Sept. 20, 95

KOREA ELECTRIC POWER CORPORATION
YGN 1 & 2 FSAR

INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(Sheet 2 of 18)

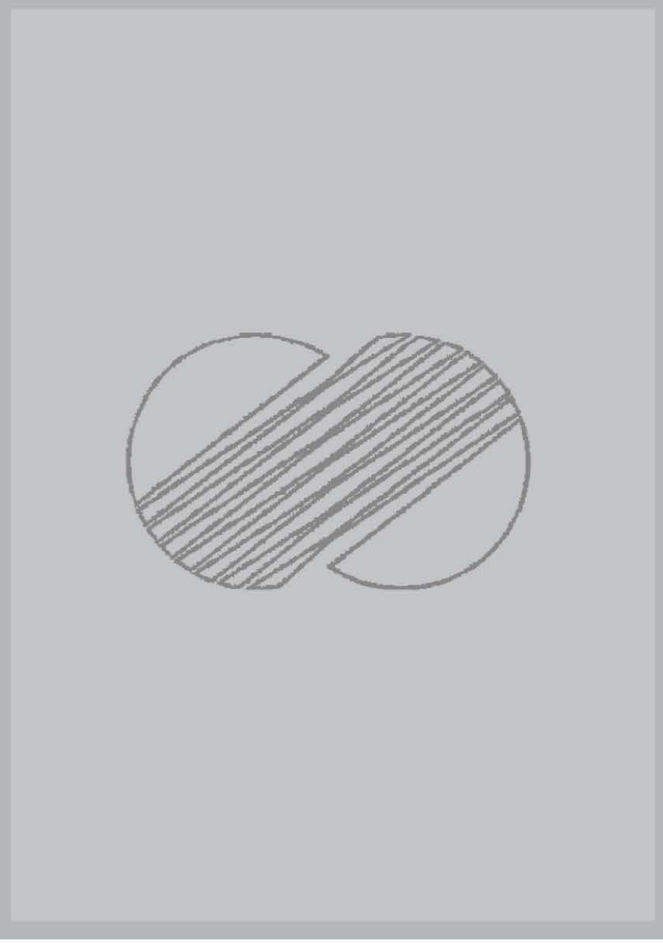
Figure 7.2-1



Amendment 105
2000.4.20

KOREA ELECTRIC POWER CORPORATION
YGN 1 & 2 FSAR

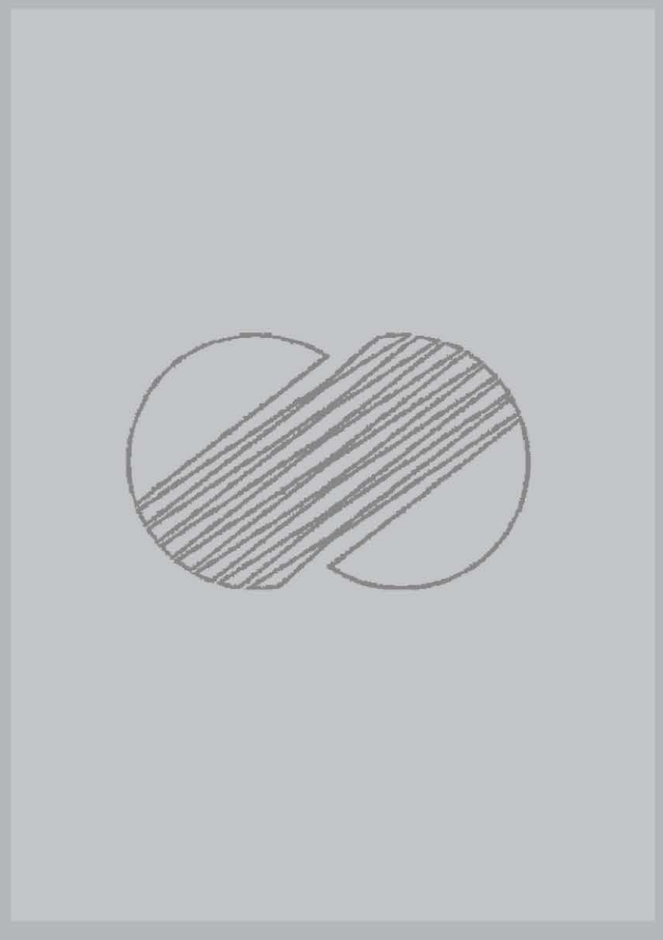
INSTUMENTATION AND CONTROL
SYSTEM DIAGRAM
(Sheet 3 Of 18)
Figure 7.2-1



KOREA ELECTRIC POWER CORPORATION
YGN 1 & 2 FSAR

INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(Sheet 4 of 18)

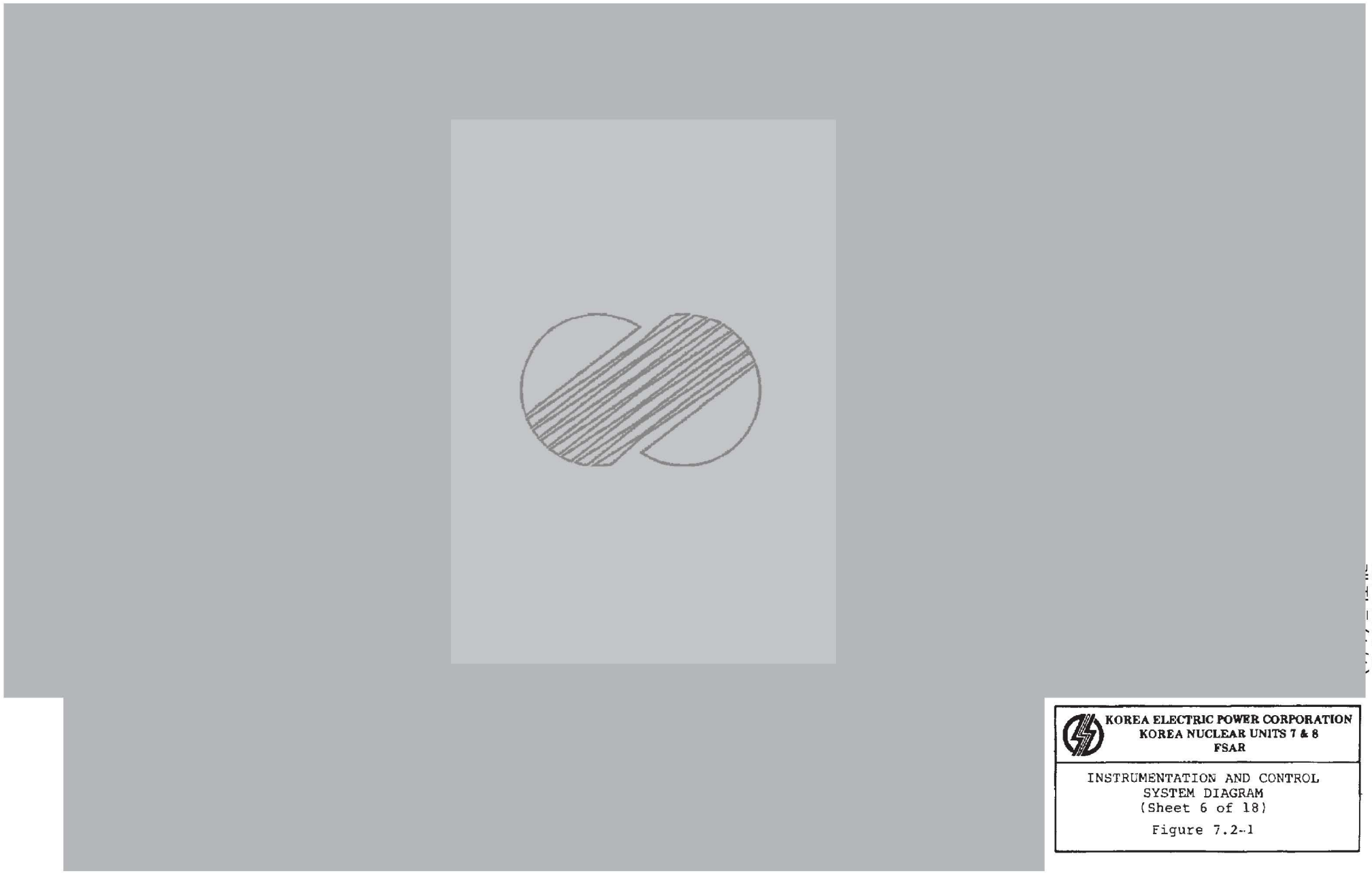
Figure 7.2-1



KOREA ELECTRIC POWER CORPORATION
KOREA NUCLEAR UNITS 7 & 8
FSAR

INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(Sheet 5 of 18)

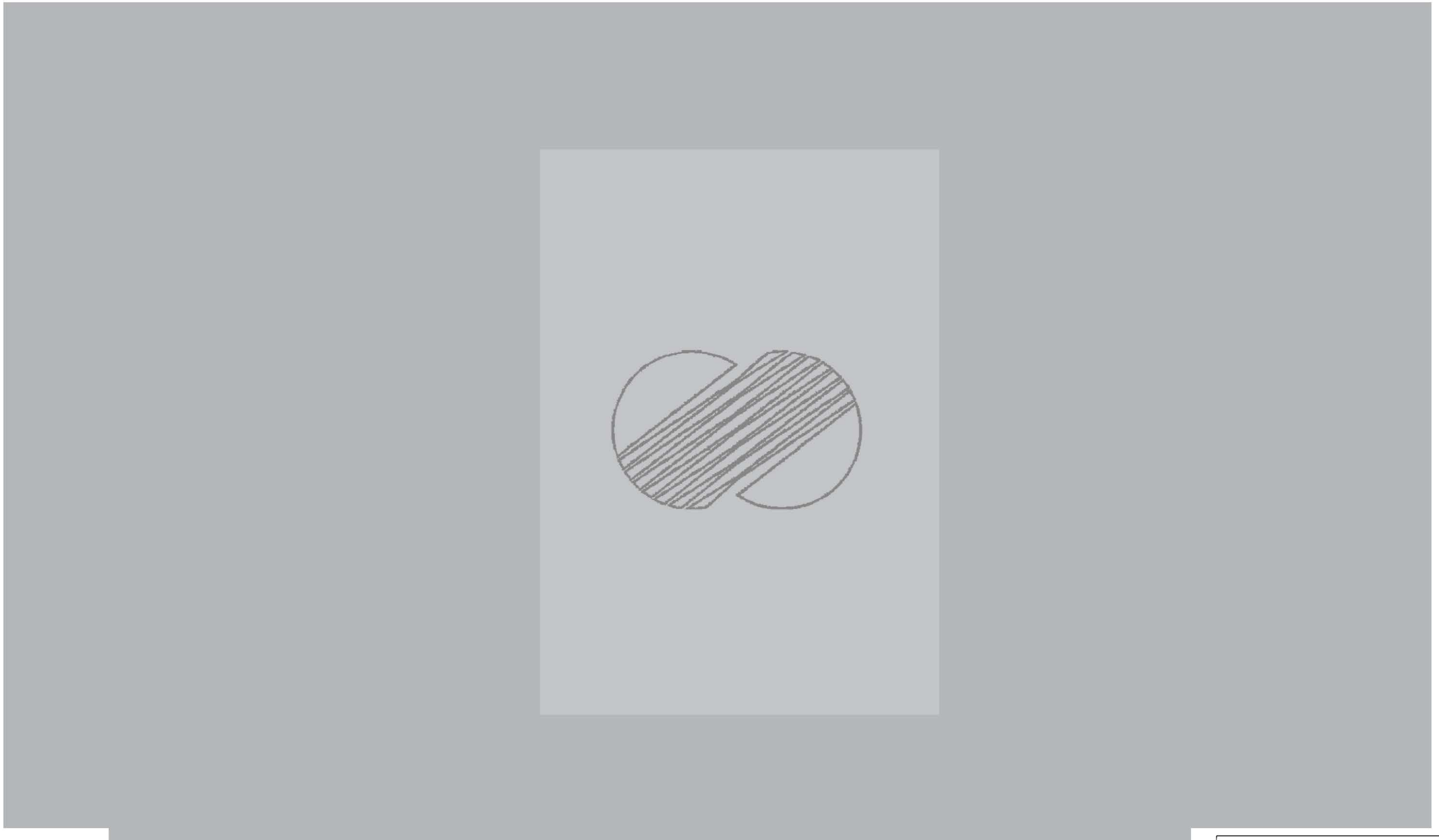
Figure 7.2-1



KOREA ELECTRIC POWER CORPORATION
KOREA NUCLEAR UNITS 7 & 8
FSAR

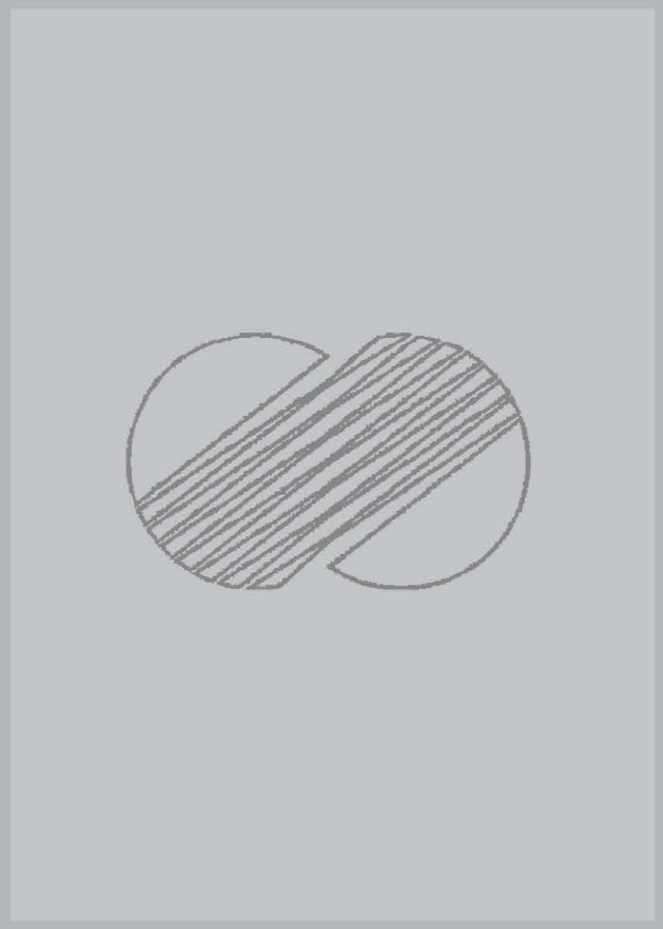
INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(Sheet 6 of 18)

Figure 7.2-1



KOREA HYDRO & NUCLEAR POWER COMPANY
YGN 1 & 2 FSAR

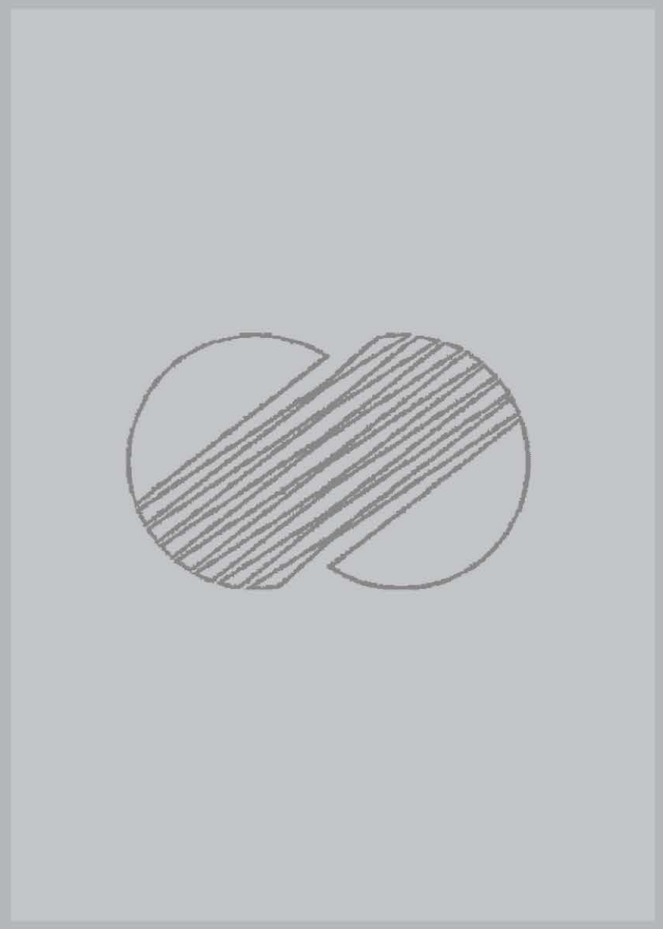
INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(SHEET 7 OF 18)
FIGURE 7.2-1



KOREA ELECTRIC POWER CORPORATION
KOREA NUCLEAR UNITS 7 & 8
FSAR

INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(Sheet 8 of 18)

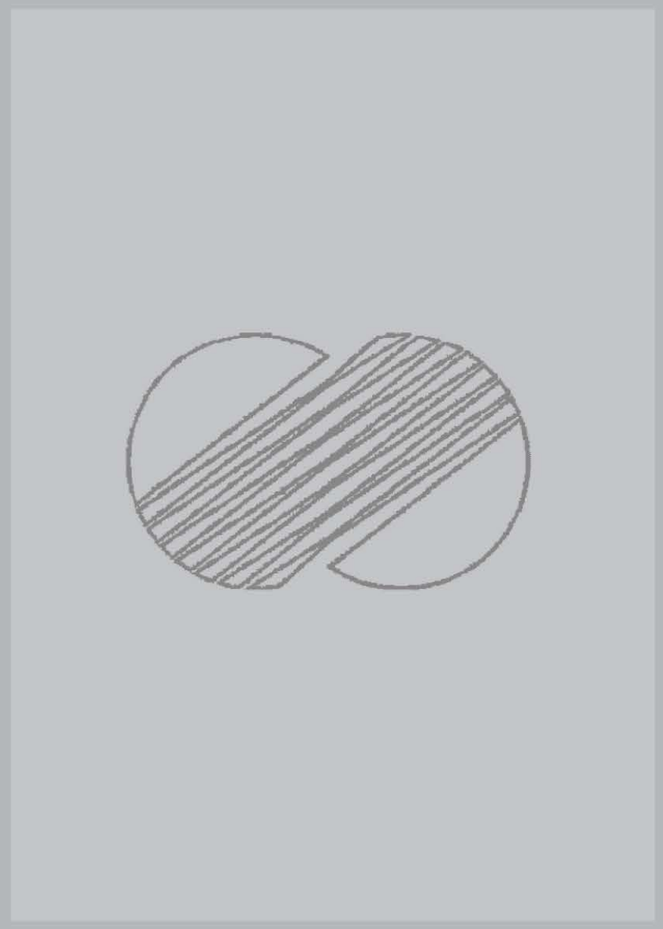
Figure 7.2-1



KOREA ELECTRIC POWER CORPORATION
YGN 1 & 2 FSAR

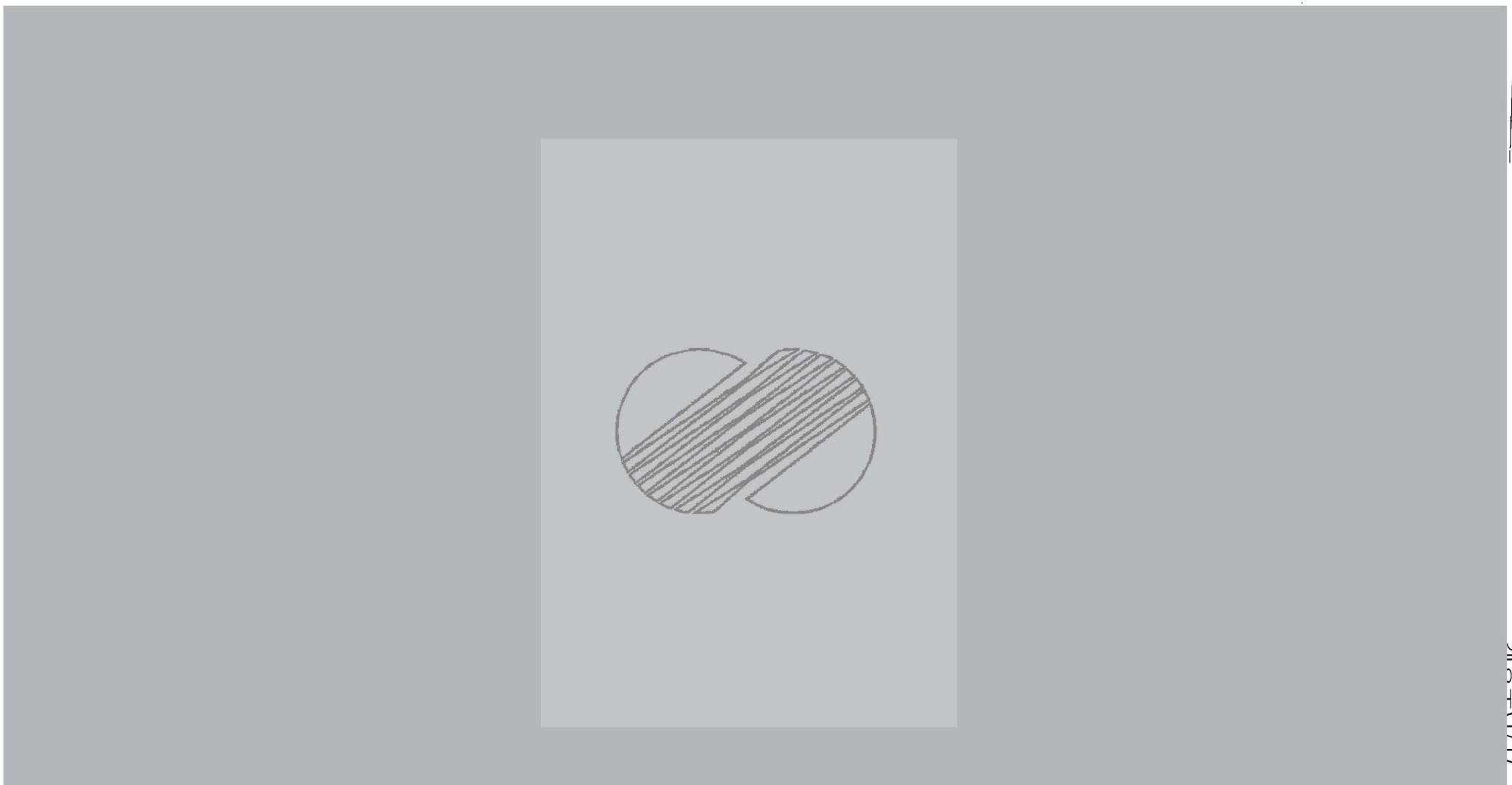
INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(Sheet 9 of 18)
Figure 7.2-1

Amendment 123
2000. 10. 24



KOREA ELECTRIC POWER CORPORATION
YGN 1 & 2 FSAR

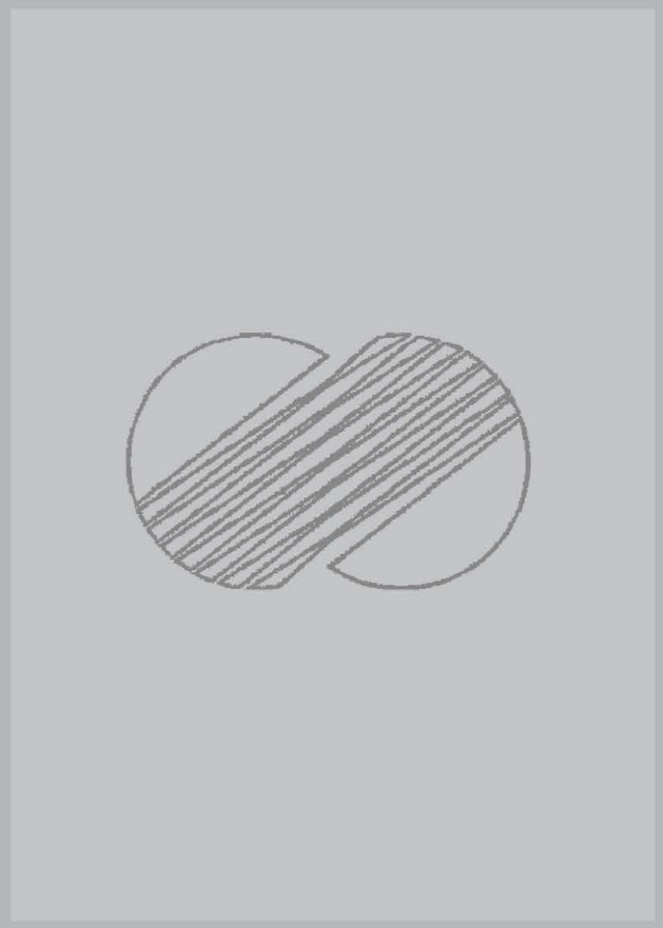
INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(Sheet 10 of 18)
Figure 7.2-1



KOREA ELECTRIC POWER CORPORATION
YGN 1 & 2 FSAR

INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(Sheet 11 of 18)
Figure 7.2-1

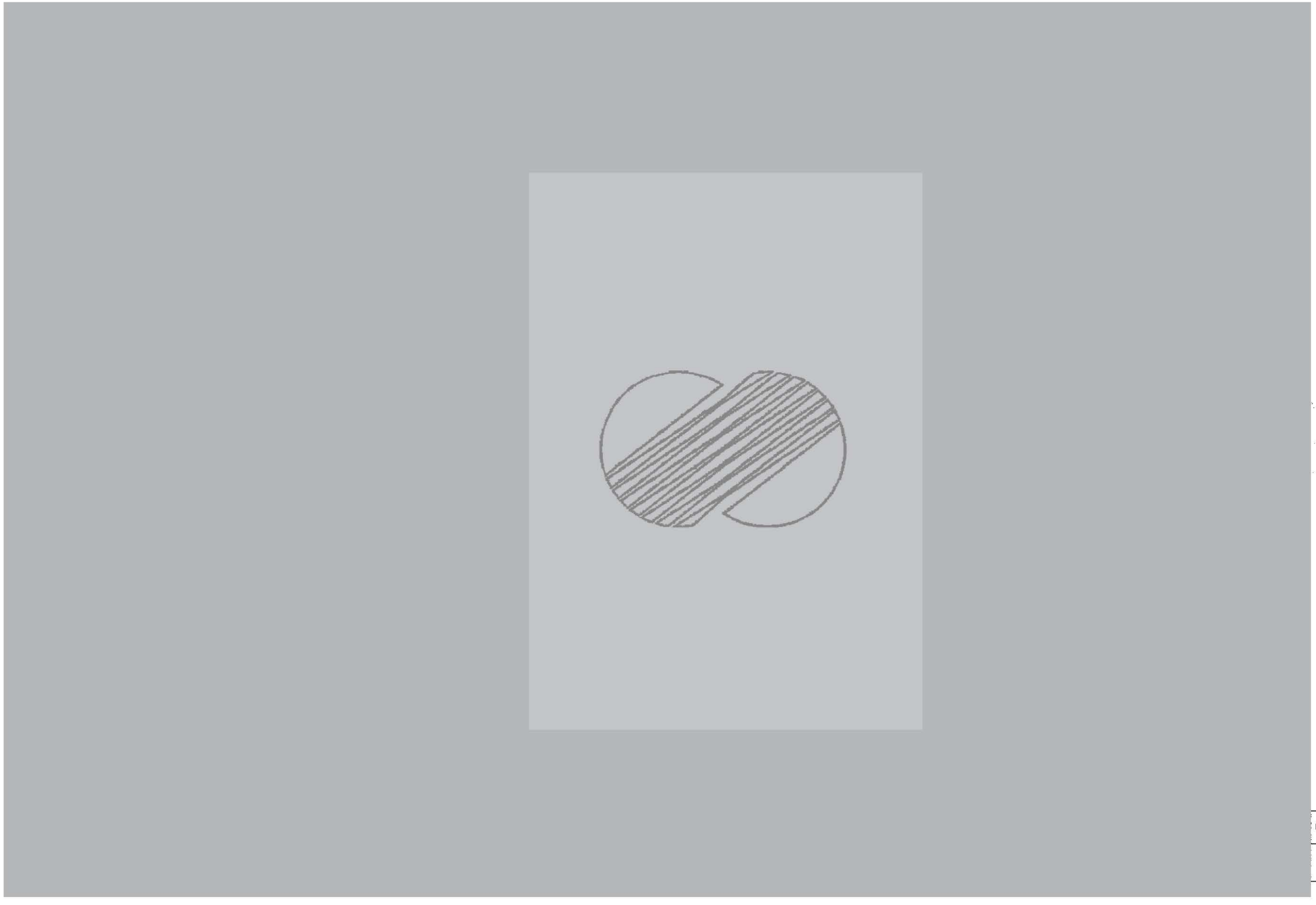
따르붙임 4
개정호(1/1)



KOREA ELECTRIC POWER CORPORATION
KOREA NUCLEAR UNITS 7 & 8
FSAR

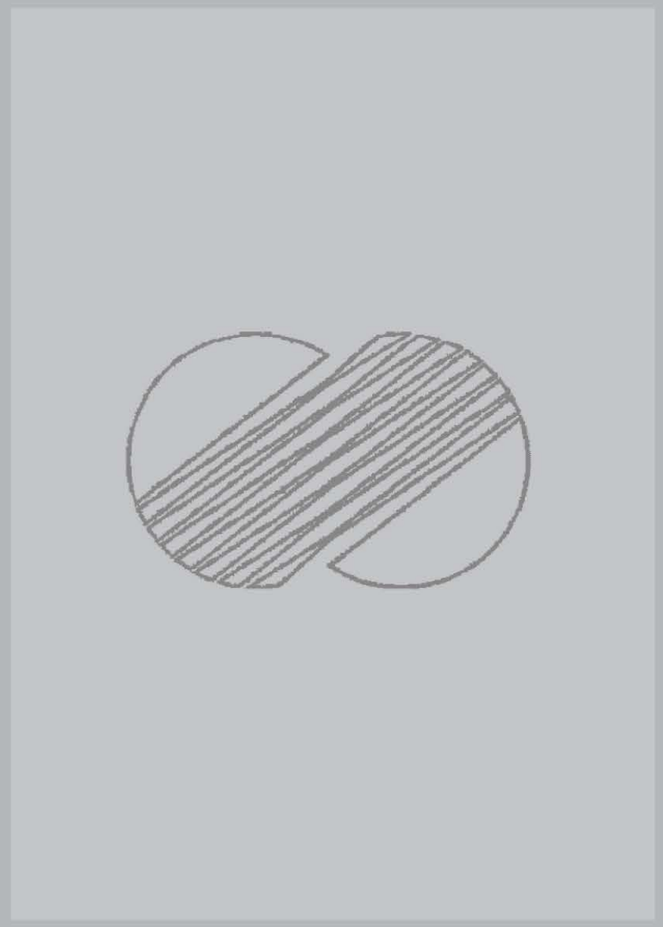
INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(Sheet 12 of 18)

Figure 7.2-1



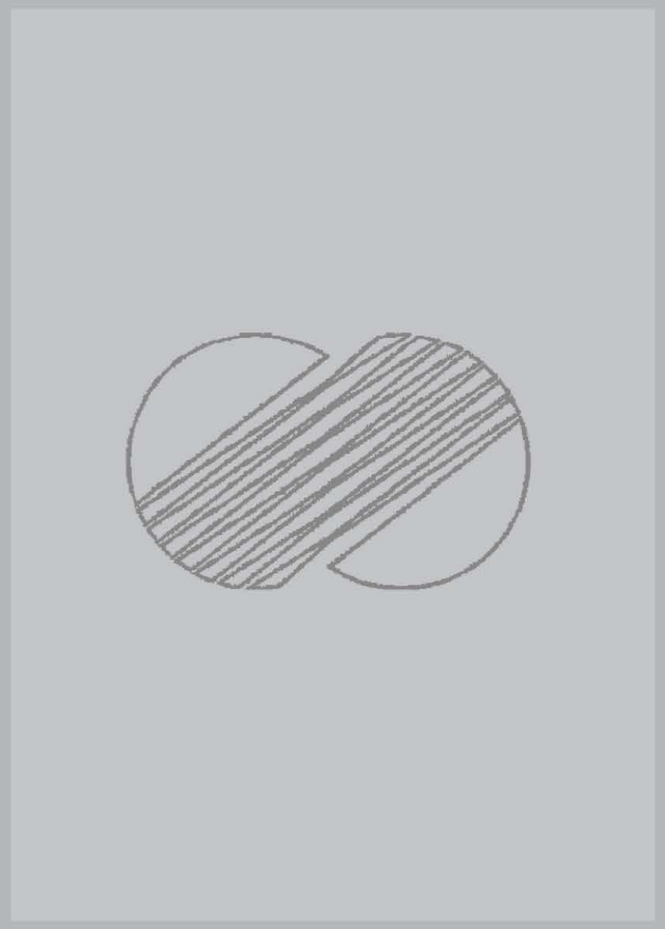
KOREA HYDRO & NUCLEAR POWER CO.
YGN 1& 2 FSAR

INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(SHEET 13 OF 18)
FIGURE 7.2-1



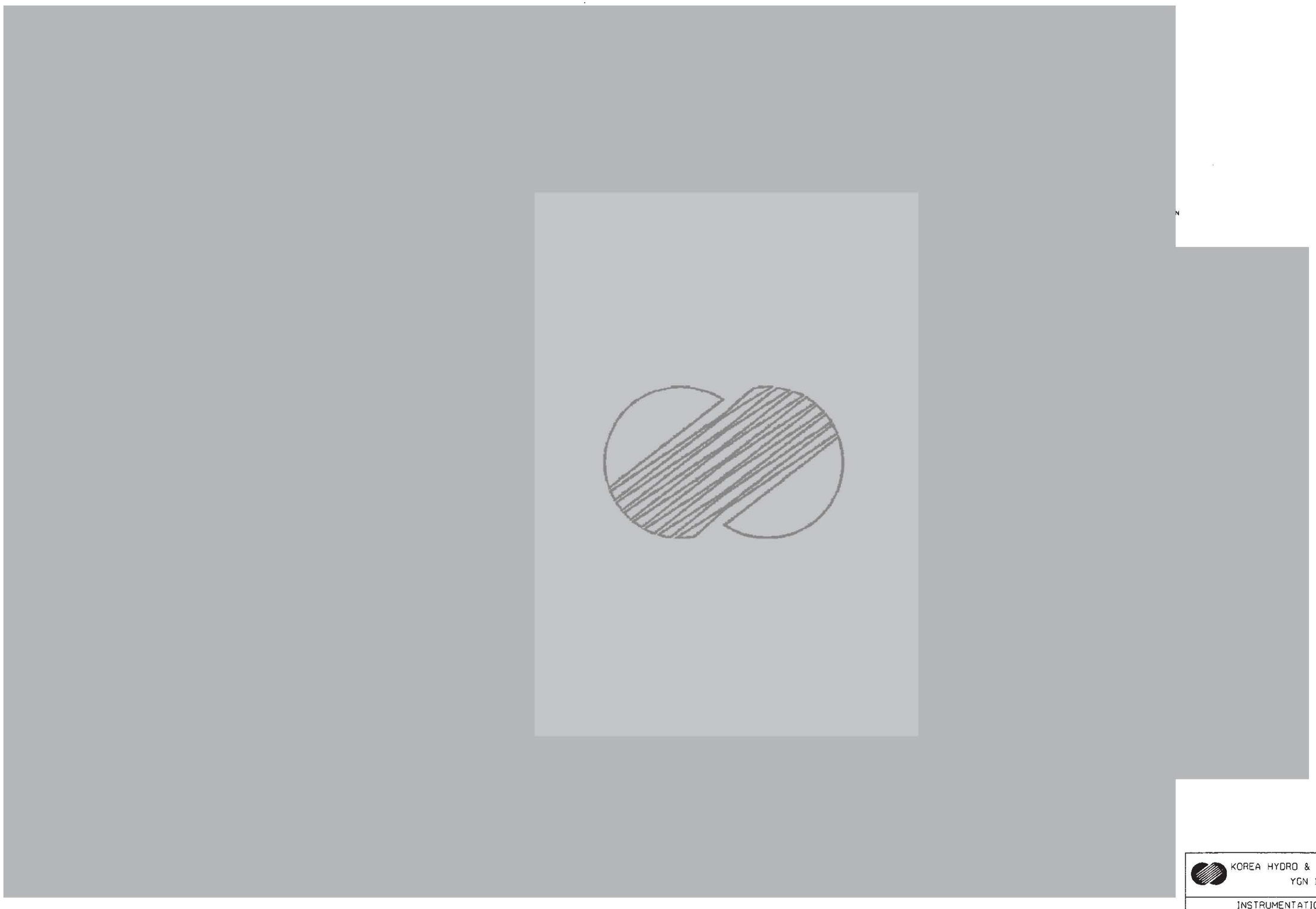
KOREA HYDRO & NUCLEAR POWER CO.
YGN 1 & 2 FSAR

INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(SHEET 14 OF 18)
FIGURE 7.2-1



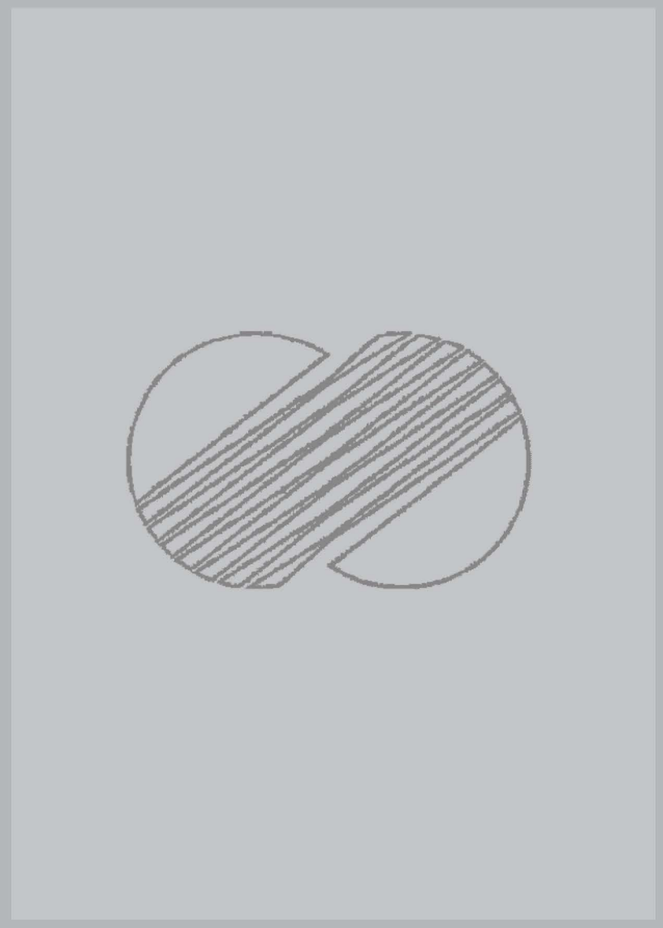
KOREA HYDRO & NUCLEAR POWER COMPANY
YGN 1 & 2 FSAR

INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(SHEET 15 OF 18)
FIGURE 7.2-1



KOREA HYDRO & NUCLEAR POWER COMPANY
YGN 1 & 2 FSAR

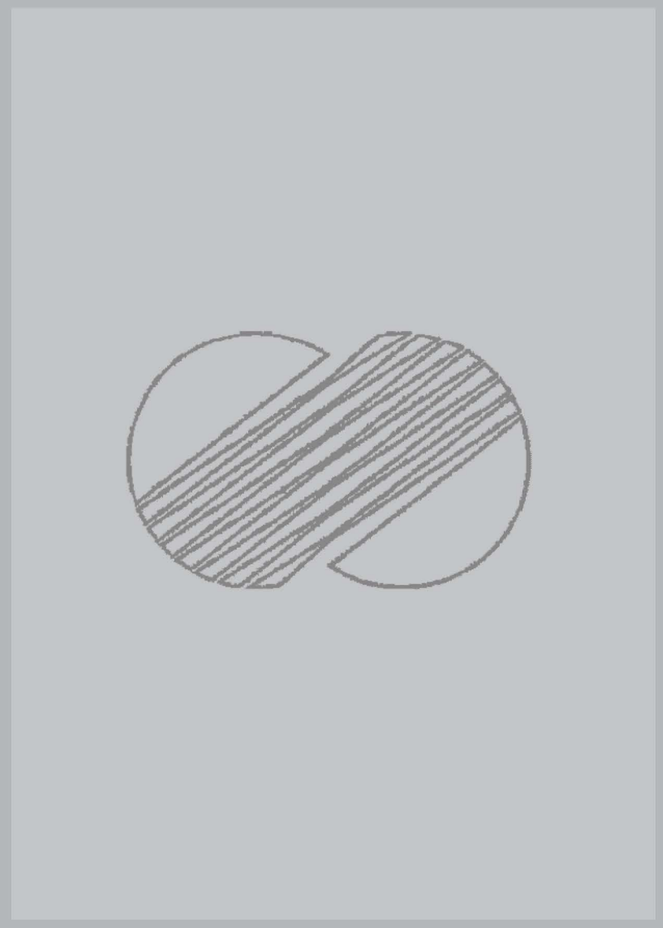
INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(SHEET 16 OF 18)
FIGURE 7.2-1



KOREA ELECTRIC POWER CORPORATION
KOREA NUCLEAR UNITS 7 & 8
FSAR

INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(Sheet 17 of 18)

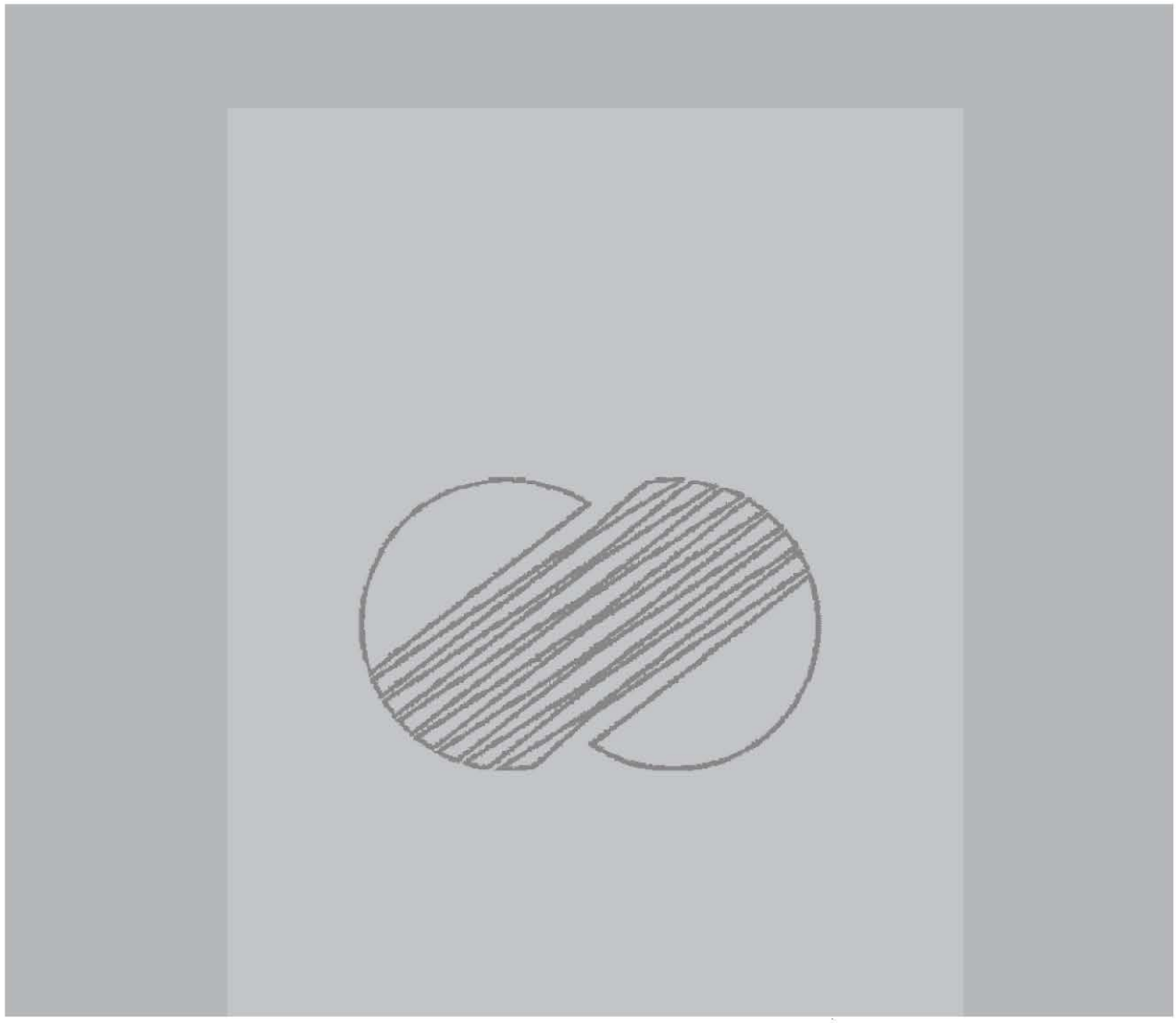
Figure 7.2-1



KOREA ELECTRIC POWER CORPORATION
KOREA NUCLEAR UNITS 7 & 8
FSAR

INSTRUMENTATION AND CONTROL
SYSTEM DIAGRAM
(Sheet 18 of 18)

Figure 7.2-1

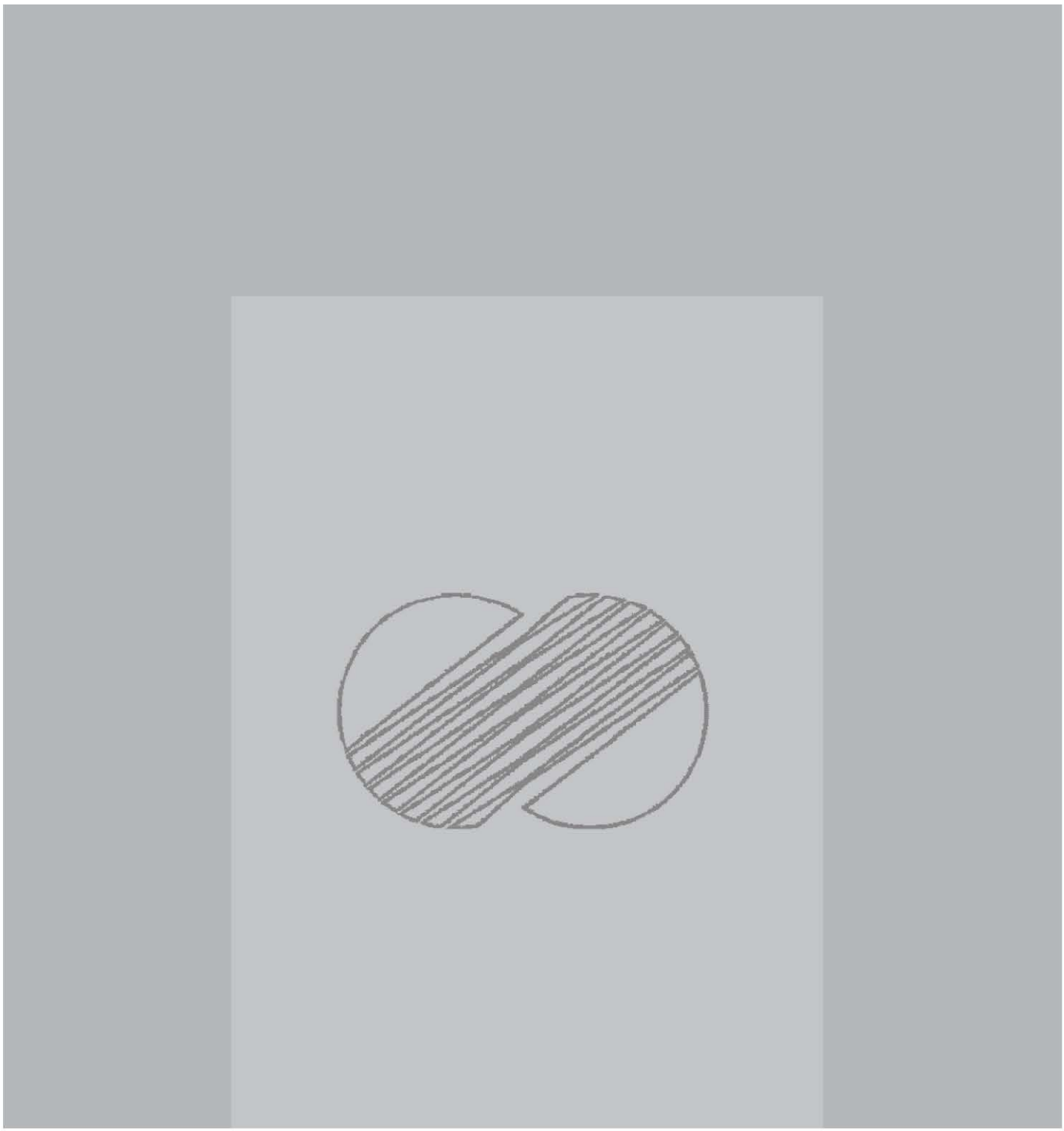


KOREA ELECTRIC POWER CORPORATION
KOREA NUCLEAR UNITS 7 & 8
FSAR

SETPOINT REDUCTION FUNCTION FOR OVERTEMPERATURE ΔT TRIPS

Figure 7.2-2

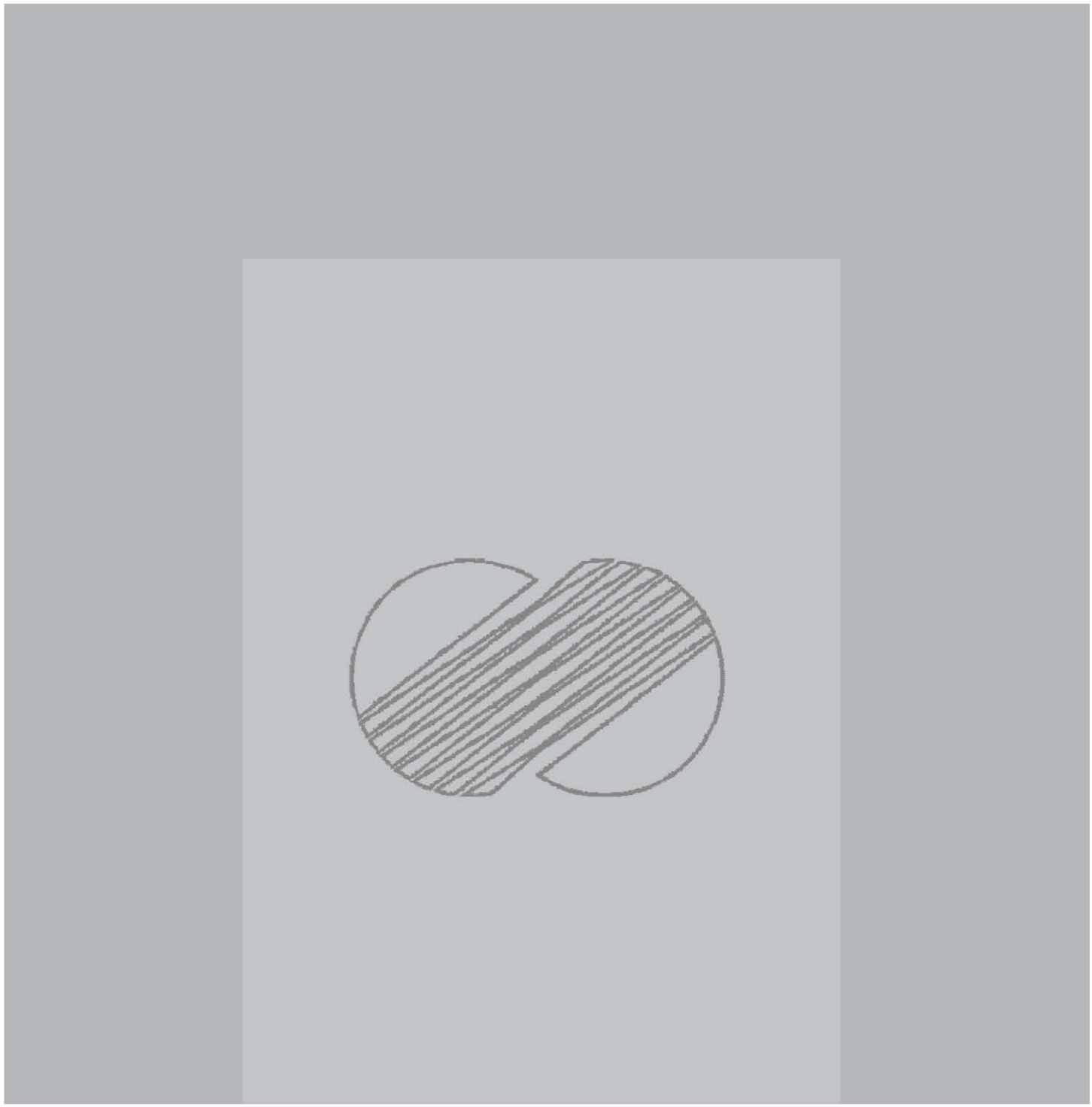
9753



KOREA ELECTRIC POWER CORPORATION
KOREA NUCLEAR UNITS 7 & 8
FSAR

PRELIMINARY ILLUSTRATION OF
OVERPOWER AND OVERTEMPERATURE
ΔT PROTECTION

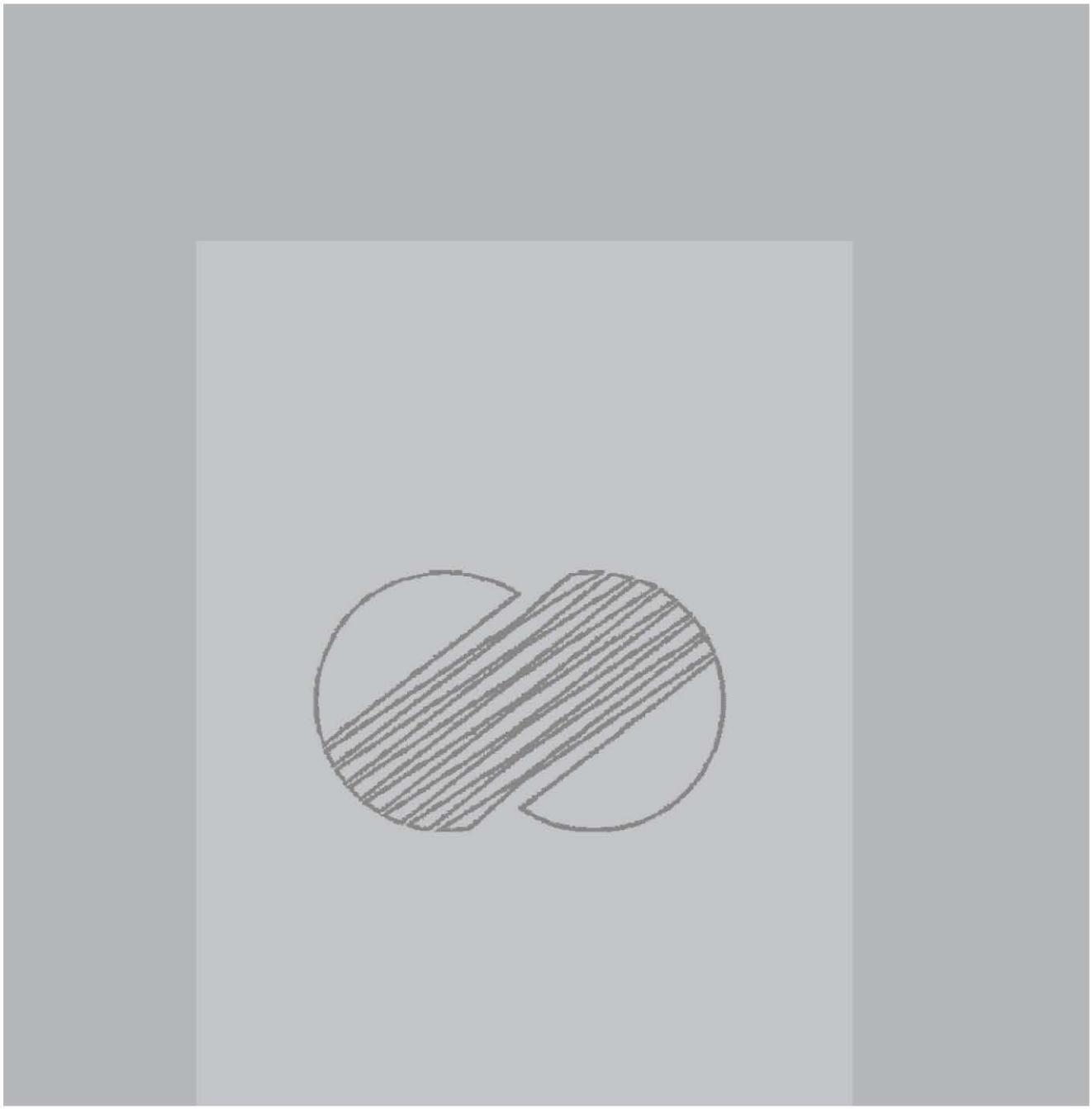
Figure 7.2-3



KOREA ELECTRIC POWER CORPORATION
KOREA NUCLEAR UNITS 7 & 8
FSAR

PRELIMINARY ILLUSTRATION OF
OVERPOWER AND OVERTEMPERATURE
ΔT PROTECTION

Figure 7.2-3



KOREA ELECTRIC POWER CORPORATION
KOREA NUCLEAR UNITS 7 & 8
FSAR

DESIGN TO ACHIEVE ISOLATION
BETWEEN CHANNELS

Figure 7.2-4

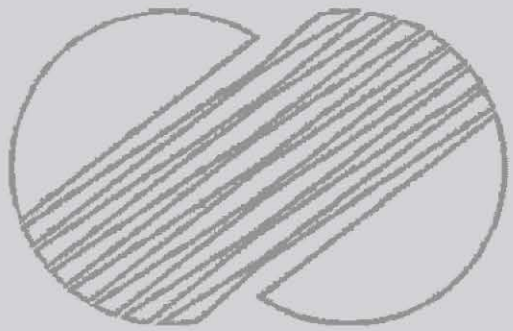


Table 7.2-1

LIST OF REACTOR TRIPS (Sheet 1 of 2)

Reactor Trip	Coincidence Logic	Interlocks	Comments
1. High neutron flux (power range)	2/4	Manual block of low setting permitted by P-10	High and low setting; manual block and automatic reset of low setting by P-10
2. Intermediate range high neutron flux	1/2	Manual block permitted by P-10	Manual block and automatic reset
3. Source range high neutron flux	1/2	Manual block permitted by P-6, interlocked with P-10	Manual block and automatic reset; automatic block above P-10
4. Power range high positive neutron flux rate	2/4	No interlocks	
5. [DELETE]			
6. Overtemperature ΔT	2/3	No interlocks	
7. Overpower ΔT	2/3	No interlocks	
8. Pressurizer low pressure	2/3	Interlocked with P-7	Blocked below P-7
9. Pressurizer high pressure	2/3	No interlocks	
10. Pressurizer high water level	2/3	Interlocked with P-7	Blocked below P-7
11. Low reactor coolant flow	2/3 per loop	Interlocked with P-7 and P-8	Low flow in one loop will cause a reactor trip when above P-8; blocked below P-8. A low flow in two loop will cause a reactor trip when above P-7; blocked below P-7.
12. Rector coolant pump undervoltage	2/3	Interlocked with P-7	Low voltage permitted below P-7
13. Reactor coolant pump underfrequency	2/3	Interlocked with P-7	Underfrequeacy on 2 pump motors will trip all reactor coolant pump breakers and cause reactor trip; reactor trip blocked blow p-7.

Table 7.2-1

LIST OF REACTOR TRIPS (Sheet 2 of 2)

Reactor Trip	Coincidence Logic	Interlocks	Comments
14. Low-low steam generator water level	2/4 per loop	No interlocks	
15. Safety injection signal	Coincident with actuation of safety injection	No interlocks	(See section 7.3 for Engineered Safety Features actuation conditions)
16. Turbine generator trip (anticipatory)			
a) Low emergency trip fluid pressure	2/3	Interlocked with P-9	Blocked below P-9
b) Closure of 4/4 turbine high pressure stop valves	4/4	Interlocked with P-9	Blocked below P-9
17. Manual	1/2	No interlocks	

Table 7.2-2

INTERLOCKS FOR REACTOR TRIP SYSTEM (Sheet 1 of 2)

Designation	Condition and Derivation	Function
	I Power Escalation Permissives	
P-6	Presence of P-6: 1/2 neutron flux (intermediate range) above setpoint	Allows manual block of source range reactor trip
	Absence of P-6: 2/2 neutron flux (intermediate range) below setpoint	Defeats the block of source range reactor trip
P-10	Presence of P-10: 2/4 neutron flux (power range) above setpoint	Allows manual block of power range (low set-range) point) reactor trip
		Allows manual block of intermediate range reactor trip and intermediate range rod stops (C-1)
		Blocks source range reactor trip (backup for P-6)
		Input to P-7
		Defeats the block of power range (low set-point) reactor trip
	Absence of P-10: 3/4 neutron flux (power range) below setpoint	Defeats the block of intermediate range reactor trip and nter-mediate range rod stops (C-1) input to P-7

Table 7.2-2

INTERLOCKS FOR REACTOR TRIP SYSTEM (Sheet 2 of 2)

Designation	Condition and Derivation	Function	
	II Blocks of Reactor Trips		
P-7	Absence of P-7: 3/4 neutron flux (power range) below setpoint (from P-10) and 2/2 turbine impulse chamber pressure below setpoint (from P-13)	Blocks reactor trip on low reactor coolant flow in more than one loop, undervoltage, underfrequency, pressurizer low pressure, and pressurizer high level	31
P-8	Absence of P-8: 3/4 neutron flux (power range) below setpoint	Blocks reactor trip on low reactor coolant flow in a single loop or turbine trip Input to P-7	31
P-13	2/2 turbine impulse chamber pressure below setpoint		

Table 7.2-3
REACTOR TRIP SYSTEM INSTRUMENTATION (Sheet 1 of 2)

Reactor Trip signal	Range	Accuracy[NOTE1]	Typical Time Responses (sec)
1. Power range high neutron flux	1 to 120% full power	± 1% of full power	0.5
2. Intermediate range high neutron flux	8 decades of neutron flux overlapping source range by 2 decades and including 100% power	Delete Delete ± 0.5% to full scale Delete	Not Applicable
3. Source range high neutron flux	6 decades of neutron flux (1 to 10^6 counts/s)	±0.5% of full scale	Not Applicable
4. Power range high positive neutron flux rate	2 to 30% of full power	±0.5% of full scale	0.5
5. [DELETE]			
6. Overtemperature △T :	T_H 530.6 to 649.4°F T_C 510.8 to 629.6°F T_{AVG} 530.6 to 629.6°F P_{PRZR} 1706.8 to 2560.2 psi (FΔΦ) −60 to +60 ΔT Setpoint 0 to 100°F	±0.5% ΔT Span	8.0
7. Overpower △T	See overtemperature ΔT	±0.5% ΔT Span	8.0
8. Pressurizer low pressure	1706.8 to 2560.2 psi	±4.3psi (compensated signal)	2.0
9. Pressurizer high pressure	1706.8 to 2560.2 psi	±4.3psi(non-compensated signal)	2.0
10. Pressurizer high water level	Entire cylindrical portion of pressurizer	±0.5% of full range ΔP between taps at design temperature and pressure	Not Applicable

362
479
123
479
362

Table 7.2-3

REACTOR TRIP SYSTEM INSTRUMENTATION (Sheet 2 of 2)

Reactor Trip signal	Range	Accuracy[Note1]	Typical Time Responses (sec)	
11. Low reactor coolant flow	0 to 120% of rated flow	±0.5% of full flow within range of 70% to 100% of full flow	1.0	
12. Reactor coolant pump undervoltage	0 to 100% rated voltage	± 1% of setting	1.5	479
13. Reactor coolant pump underfrequency	54 to 60 Hz	± 0.1 Hz	0.6	
14. Low-low steam generator	±~ 6 ft. from nominal full load water level	0.5% of ΔP signal over pressure range of 700 to 1200 psig	2.5	479
15. Turbine trip			Not Applicable	479

Note 1 : Rack Calibration Accuracy

Table 7.2-4

REACTOR TRIP CORRELATION (Sheet 1 of 6)

Trip	Accident (a)	Tech. Spec. (b)
1. Power range high neutron flux trip (low setpoint)	1. Uncontrolled rod cluster control assembly bank withdrawal from a subcritical condition (15.4.1) 2 Excessive heat removal due to feedwater system malfunctions (15.1.1, 15.1.2) 3. Rupture of a control rod drive mechanism housing (rod cluster control assembly ejection) (15.4.8)	ITS Chapter 1 table 3.3.1-1
2. Power range high neutron flux trip (high setpoint)	1. Uncontrolled rod cluster control assembly bank withdrawal from a subcritical condition (15.4.1) 2. Uncontrolled rod cluster control assembly bank withdrawal at power (15.4.2) 3. Startup of an inactive reactor coolant loop (15.4.4) 4. Excessive heat removal due to feedwater system malfunctions (15.1.1, 15.1.2)	ITS Chapter 1 table 3.3.1-1

Table 7.2-4

REACTOR TRIP CORRELATION (Sheet 2 of 6)

Trip	Accident (a)	Tech. Spec. (b)
	5. Excessive load increase incident (15.1.3)	
	6. Accidental depressurization of the main steam system (15.1.4)	
	7. Major secondary system pipe ruptures (15.1.5)	
	8. Rupture of a control rod drive mechanism housing (rod cluster control assembly ejection) (15.4.8)	
3. Intermediate range high neutron flux (15.4.1)	1. Uncontrolled rod cluster control assembly bank withdrawal from a trip subcritical condition	See note (c)
4. Source range high neutron flux trip	1. Uncontrolled rod cluster control assembly bank withtdrawal from a subcritical condition (15.4.1)	See note (c)
5. Power range high positive neutron flux rate trip	1. Rupture of a control rod drive mechanism housing (rod cluster control assembly ejection) (15.4.8)	ITS Chapter 1 table 3.3.1-1
6. [DELETE]		

Table 7.2-4

REACTOR TRIP CORRELATION (Sheet 3 of 6)

Trip	Accident (a)	Tech. Spec. (b)
7. Overtemperature ΔT trip	1. Uncontrolled rod cluster control assembly bank withdrawal at power (15.4.2)	ITS Chapter 1 table 3.3.1-1
	2. Uncontrolled boron dilution (15.4.6)	
	3. Loss of external electrical load and/or turbine trip (15.2.2, 15.2.3, 15.2.5)	
	4. Excessive heat removal due to feedwater system malfunctions (15.2.1, 15.1.3)	
	5. Excessive load increase incident (15.1.3)	
	6. Accidentsl depressuriza-tion of the RCS (15.6.1)	
	7. Accidental depressuri-zation of the main steam system (15.1.4)	
	8. Loss of reactor coolant from small ruptured pipes or from cracks i n large piped which actuates ECCS (15.6.2)	
8. Overpower ΔT trip	1. Uncontrolled rod cluster control assembly bank withdrawal at power (15.4.2)	ITS Chapter 1 table 3.3.1-1
	2. Excessive heat removal due to feedwater system malfunctions (15.1.1, 15.1.2)	

Table 7.2-4

REACTOR TRIP CORRELATION (Sheet 4 of 6)

Trip	Accident (a)	Tech. Spec. (b)	
	3. Excessive load increase incident (15.1.3)		
	4. Accidental depressurization of the main steam system (15.1.4)		
	5. Major secondary system pipe ruptures (15.1.5)		
9. Pressurizer low pressure trip	1. Accidental depressurization of the RCS (15.6.1)	ITS Chapter 1 table 3.3.1-1	648
	2. Loss of reactor coolant from small ruptured pipes or from cracks in large pipes which actuates ECCS (15.6.2)		
	3. Major reactor coolant system pipe ruptures (LOCA) (15.6.5)		
	4. Steam generator tube rupture (15.6.3)		
10. Pressurizer high pressure trip	1. Uncontrolled rod cluster control assembly bank withdrawal at power (15.4.2)	ITS Chapter 1 table 3.3.1-1	648
	2. Loss of external electrical load and/or turbine trip (15.2.2. 15.2.3. 15.2.5)		
11. Pressurizer high water level trip	1. Uncontrolled rod cluster control assembly bank withdrawal at power (15.4.2)	ITS Chapter 1 table 3.3.1-1	648

Table 7.2-4

REACTOR TRIP CORRELATION (Sheet 5 of 6)

Trip	Accident (a)	Tech. Spec. (b)
	2. Loss of external electrical load and/or turbine trip (15.2.2, 15.2.3, 15.2.5)	
12. Low reactor coolant flow	1. Partial loss of forced reactor coolant flow (15.3.1)	ITS Chapter 1 table 3.3.1-1
	2. Loss of offsite power to the station auxiliaries (station blackout) (15.2.6)	
	3. Complete loss of forced reactor coolant flow (15.3.2)	
13. Reactor coolant pump under-voltage trip	1. Complete loss of forced reactor coolant flow (15.3.2)	ITS Chapter 1 table 3.3.1-1
14. Reactor coolant pump bus under-frequency trip	1. Complete loss of forced reactor coolant flow (15.3.2)	ITS Chapter 1 table 3.3.1-1
15. Low-low steam generator water level trip	1. Loss of normal feedwater (15.2.7)	ITS Chapter 1 table 3.3.1-1
16. Reactor trip on turbine trip	1. Loss of external electrical load and/or turbine trip (15.2.2, 15.2.3, 15.2.5)	See note (c)
	2. Loss of offsite power to the station auxiliaries (station blackout) (15.2.6)	See note (c)

Table 7.2-4

REACTOR TRIP CORRELATION (Sheet 6 of 6)

Trip	Accident (a)	Tech. Spec. (b)
17. Safety injection signal actuation trip	1. Accidental depressurization of the main steam system (15.1.4)	See note (d)
18. Manual trip	Available for all accidents (chapter 15)	See note (c)

NOTES:

a. References refer to accident analyses presented in chapter 15.

b. References refer to technical specifications presented in ITS Chapter 1. | 348

C. A technical specification is not required because this trip is not assumed to function in the accident analyses.

d. Accident assumes that the reactor is tripped at end of life (EOL) which is the worst initial condition for this case. Pressurizer low pressure is the initial trip of safety injection.

7.3 ENGINEERED SAFETY FEATURE SYSTEMS

In addition to the requirements for a reactor trip for anticipated abnormal transients, adequate instrumentation and controls are provided to sense accident situations and initiate the operation of necessary engineered safety features (ESF). The occurrence of a limiting fault, such as a loss-of-coolant accident (LOCA) or a steam line break, requires a reactor trip plus actuation of one or more of the ESF in order to prevent or mitigate damage to the core and reactor coolant system (RCS) components, and ensure containment integrity.

In order to accomplish these design objectives, the engineered safety features actuation system (ESFAS) shall have proper and timely initiating signals that are to be supplied by the sensors, transmitters, and logic components making up the various instrumentation channels of the ESFAS.

7.3.1 DESCRIPTION

The ESFAS monitors selected nuclear steam supply system (NSSS) and balance of plant (BOP) parameters to sense accident situations and initiate the operation of necessary ESF systems in order to prevent or mitigate damage to the core and RCS components and ensure containment integrity.

The ESFAS uses selected plant parameters, determines whether or not predetermined safety limits are being exceeded and, if they are, combines the signals into logic matrices sensitive to combinations indicative of primary or secondary system boundary ruptures (ANS Condition III or IV events). Once the required logic combination is completed, the system sends actuation signals to the appropriate ESF components.

The ESFAS meets the functional requirements of General Design Criteria 13, 20, 27 and 28 of 10 CFR 50, Appendix A.

The occurrence of a limiting fault, such as a LOCA or a steam line break, requires a reactor trip plus actuation of one or more of the ESF in order to prevent or mitigate damage to the core and RCS components, and ensure containment integrity.

The ESFAS can be divided as follows:

A. NSSS ESFAS

B. BOP ESFAS.

7.3.1.1 System Description

7.3.1.1.1 NSSS ESFAS

The NSSS ESFAS is designed and furnished by Westinghouse with the NSSS.

The NSSS ESFAS provides the following actuation signals:

A. Safety injection signal (SIS)

B. Containment isolation signal phase A (CIS-A)

C. Containment spray signal (CSS)

D. Containment isolation signal phase B (CIS-B)

E. Feedwater isolation signal (FWIS).

The NSSS ESFAS provides also the following signals which are utilized for the generation of some of the BOP ESFAS actuation signals:

A. Steam pressure rate high signal

B. Steam line pressure low signal

C. Containment pressure high (Hi-2) signal

D. Steam generator water level low-low signal.

The NSSS ESFAS consists of two discrete portions of circuitry: (1) an analog portion consisting of three to four redundant channels per parameter or variable to monitor various plant parameters such as the steam generator pressures, and water levels and the RCS pressurizer pressure, and containment pressures; and (2) a digital portion consisting of two redundant logic trains that receive inputs from the analog protection channels and perform the logic needed to actuate the ESF. Each digital actuation train is capable of actuating the minimum ESF equipment required, thereby assuring that any single failure within either of the redundant trains shall not result in defeat of the required protective function.

The redundant concept is applied to both the analog and logic portions of the system. Separation of redundant analog channels, begins at the process sensors, and is maintained in the field wiring, containment vessel penetrations, and analog protection

racks terminating at the redundant groups of logic racks. The design meets the requirements of General Design Criteria 20, 21, 22, 23, and 24 of 10 CFR 50, Appendix A.

The variables are sensed by analog circuitry as discussed in reference 1 and in section 7.2. The outputs from the analog channels are combined into actuation logic as shown in figure 7.2-1, sheets 5, 6, 7, and 8. Table 7.3-1 gives additional information pertaining to logic and function. Figure 7.3-10 shows a typical block diagram of NSSS ESFAS signals.

The interlocks associated with the NSSS ESFAS are outlined in table 7.3-2. These interlocks satisfy the functional requirements discussed in subsection 7.1.2.

7.3.1.1.2 BOP ESFAS

The BOP ESFAS designed and furnished by the BOP designer are housed in the solid-state interposing logic system cabinets.

The BOP ESFAS consist of two discrete portions of circuitry: (1) an analog portion consisting of two redundant channels per parameter and (2) a digital portion consisting of two redundant logic trains which receive inputs from the analog protection channels and performs the logic needed to actuate the ESF equipment. Each digital actuation train is capable of actuating the minimum ESF equipment required, thereby assuring that any single failure within either of the redundant trains shall not result in failure of the required protective function.

The redundant concept is applied to both the analog and digital portions of the system.

The BOP ESFAS is solid-state design.

The ESFAS meets the testability requirement of USNRC Regulatory Guide 1.22.

The design meets the requirements of General Design Criteria 19, 20, 21, 22, 23 and 24 of 10 CFR 50, Appendix A.

Figure 7.3-11 shows a typical block diagram of BOP ESFAS signals.

Logic and function associated with the BOP ESFAS are outlined in table 7.3-3.

The BOP ESFAS provide the following actuation signals.

A. Fuel building emergency ventilation signal (FBEVS)

B Containment purge isolation signal (CPIS)

C. Control room emergency ventilation signal (CREVS)

D. Main steam isolation signal (MSIS)

E. Auxiliary feedwater signal - motor-driven (AFS-MD)

F. Auxiliary feedwater signal - turbine-driven (AFS-TD)

G. Diesel generator load sequencer signal.

7.3.1.1.3 System Level Manual Initiation

System level manual initiation from the main control board is provided for the following ESFAS signals:

A. Safety injection: two switches. Each switch operates both trains. Manual safety injection actuation also initiates CIS-A, FWIS, AFS-MD, diesel generator sequencer, CREVS, and CPIS.

B. Containment isolation phase A: two switches. Each switch operates both trains. Manual containment isolation phase A also initiates CPIS.

C. Containment spray actuation: four switches. Two switches are associated with each train, both of which must be operated concurrently to actuate their associated train. Manual containment spray actuation also initiates CIS-B and CPIS.

D. Fuel building emergency ventilation: two switches. Each switch operates both trains. Manual fuel building emergency ventilation actuation also initiates CREVS.

E. Control room emergency ventilation: two switches. Each switch operates both trains.

F. Main steam line isolation: two switches. Each switch operates both trains.

G. Auxiliary feedwater: motor-driven, two switches. Each switch operates both trains.

H. Auxiliary feedwater: turbine-driven, two switches. Each switch operates both trains.

Manual control switches are also provided at the component level to complete the switchover from the injection to the recirculation phase after a LOCA.

7.3.1.1.4 Function Initiation

7.3.1.1.4.1 N3S3 ESFAS. The specific functions that rely on the N3S3 ESFAS for initiation are:

A. Reactor trip, provided that this trip has not already been generated by the reactor trip system

B. Safety Injection Signal (SIS)
The SIS is originated by the following signals (see table 7.3-1, item 1):

1. Containment pressure high (Hi-1)

2. Low steam line pressure in two-out-of-three channel signals below the set point in any one loop.

3. Pressurizer pressure low

4. Manual from the control board.

The following equipment is actuated by the safety injection signal:

1. Cold leg injection isolation valves that are opened for injection of borated water by safety injection/ charging pumps into the cold legs of the RCS.

2. Charging pumps, residual heat removal pumps, and associated valving that provide emergency makeup water to the cold legs of the RCS following a LOCA.

3. Containment fan cooler system (reduction of fan speed and shutoff of chilled water supply) that serves to cool the containment and limit the potential for release of fission products from the containment by reducing the pressure following an accident.

4. Nuclear service cooling water pumps and component cooling water pumps that serve as part of the ultimate heat sink and as part of the heat sink for containment cooling.

5. Motor-driven auxiliary feedwater pumps (via BOP ESFAS signal AFS-MD).

6. Start the diesel generators to ensure backup supply of power to emergency and supporting system components (via BOP ESFAS signal sequence).

7. Start the following emergency heating, ventilation, and air conditioning (HVAC):

   a. Auxiliary building essential HVAC
   b. Control room emergency HVAC
   c. Control building essential HVAC
   d. Fuel building emergency exhaust system
   e. Diesel generator building emergency HVAC.

8. Turbine trip to prevent or mitigate the effects of excessive RCS cooldown.

9. Stop boron injection recirculation pump and isolate boron injection tank from recirculation loop.

10. Trip main feedwater pump turbines (via feedwater isolation signal).

11. Generate the following ESFAS signals:

   a. Containment isolation signal phase A
   b. Feedwater isolation signal
   c. Containment purge isolation signal
   d. Control room emergency ventilation signal
   e. Auxiliary feedwater signal – motor-driven
   f. Diesel generator load sequencer signal.

12. Trip selected isolation breakers feeding non-Class 1E load energized from Class 1E sources.

Table 7.3A8, item 1, furnishes a detailed list of equipment activated by the SIS.

C. Containment Isolation Signal Phase A (CIS-A)

The containment isolation signal phase A is originated by the same signals that originate the SIS or manually from the control board (see table 7.3-1, item 2).

Equipment actuated by the containment isolation signal phase A are those which prevent fission products being released to the site boundary by isolating nonessential lines for reactor protection.

Table 7.3-18, item 2, furnishes a detailed list of equipment actuated by the CIS-A.

D. Containment Spray Signal (CSS)

The containment spray signal is originated by containment pressure high (Hi-3) or manually from the control board (see table 7.3-1, item 3).

The containment spray signal initiates equipment which will generate containment spray to reduce containment pressure and temperature following a LOCA or steam line break accident inside of containment.

Table 7.3-18, item 3, furnishes a detailed list of equipment activated by the CSS.

E. Containment Isolation Signal Phase B (CIS-B)

The containment isolation signal phase B is originated by containment pressure high (Hi-3) or by the manual actuation of containment spray signal (see table 7.3-1, item 4).

The containment isolation signal phase B initiates equipment that isolates certain lines penetrating the containment following a LOCA, or a steam or feedwater line break within containment to limit radioactive releases. Subsection 6.2.4 discusses isolation valves in further detail.

Table 7.3-18, item 4, furnishes a detailed list of equipment activated by the CIS-B.

F. Feedwater Isolation Signal (FWIS)

The feedwater isolation signal is originated by the same signals that originate the SIS or two-out-of-three steam generator level high-high channel signals in any steam generator (see table 7.3-1, item 5).

Equipment actuated by the feedwater isolation signal are those which are required to prevent or mitigate the effect of excessive cooldown.

Table 7.3-18, item 5, furnishes a detailed list of equipment actuated by the FWIS.

7.3.1.1.4.2 BOP ESFAS. The specific functions that rely on the BOP ESFAS for initiation are:

A. Fuel Building Emergency Ventilation Signal (FBEVS)

The fuel building emergency ventilation equipment is designed to minimize the radiation level in the fuel building by initiating two separate and redundant actuation trains in the event of high radiation in the fuel building. The signal can be initiated manually from the control board or automatically by a high radiation signal from the spent fuel pool bridge area radiation monitor or from the fuel building gaseous exhaust radiation monitor. Two separate and redundant actuation trains are initiated by the signal (see table 7.3-3, item 1). A detailed list of equipment activated by the FBEVS is shown in table 7.3-19, item 1.

B. Containment Purge Isolation Signal (CPIS)

The containment purge equipment is designed to filter containment air and to exhaust the filtered air to the atmosphere within an acceptable radiation level. The containment purge isolation signal is initiated automatically by the SIS (NSSS ESFAS) or from the containment purge ventilation exhaust radiation monitor, refueling machine bridge area radiation monitor or the containment high range area radiation monitors. Two separate and redundant actuation trains are initiated by the signal. Manual actuation of either CSS or CIS-A also initiates the CPIS (see table 7.3-3, item 2). A detailed list of equipment activated by the CPIS is shown on table 7.3-19, item 2.

This design meets the requirements of Section II.E.4.2 of NUREG-0660.

C. Control Room Emergency Ventilation Signal (CREVS)

The control room emergency ventilation equipment isolates the control room from the outside area in event of high radiation in the atmosphere.

The control room emergency ventilation signal is originated by the following signals:

1. Control room ventilation intake radiation high

2. Containment purge exhaust radiation high
3. Refueling machine bridge area radiation
4. FBEVS
5. SIS (NSSS ESFAS)
6. Manual.

Two separate and redundant actuation trains are initiated by the signal (see table 7.3-3, item 3). A detailed list of equipment activated by the CREVS is shown on table 7.3-19, item 3.

D. Main Steam Isolation Signal (MSIS)

A main steam line isolation signal can be initiated manually from the control board or automatically by one of the following signals.

1. Steam pressure rate high (two-out-of-three NSSS ESFAS channels)
2. Steam line pressure low (two-out-of-three NSSS ESFAS channels)
3. Containment pressure high Hi-2 (two-out-of-three NSSS ESFAS channels).

Two separate and redundant actuation trains are initiated by the signal (see table 7.3-3, item 4). A detailed list of equipment activated by the MSIS is shown on table 7.3-19, item 4.

E. Auxiliary Feedwater Signal - Motor-Driven (AFS-MD)

The auxiliary feedwater system is designed to provide an adequate water supply to the steam generators in the event of failure of the main feedwater pumps, a plant blackout, steam generator low-low level or ATWS Mitigation System initiation signals. The auxiliary feedwater signal - motor-driven - can be initiated manually from the control board or by one of the following signals:

216

1. Steam generator feedwater pump (SGFP) turbine trip signal (three-out-of-three channels) equivalent to trip all of main feedwater pumps
2. Two-out-of-four NSSS ESFAS steam generator low-low signal (any one-out-of-three steam generators)

3. SIS (NSSS ESFAS)

4. 4.16 kV bus low voltage from two-out-of-four channels with the diesel generator breaker closed.

216 | 5. ATWS Mitigation System initiation signals.

Two separate and redundant actuation trains are initiated by the signal (see table 7.3-3, item 5). The emergency shutdown panel (ESP) does not have the capability to initiate the auxiliary feedwater signal, motor-driven; however, control of the auxiliary feedwater system is accomplished from the ESP by individual actuation of the equipment. A detailed list of equipment activated by the AFS-MD is shown on table 7.3-19, item 5.

The design of the automatic initiation of the auxiliary feedwater system complies with Section II.E.1.2 of NUREG-0660.

F. Auxiliary Feedwater Signal - Turbine-Driven (AFS-TD)

The auxiliary feedwater signal - turbine-driven - can be initiated manually from the control board or automatically by one of the following signals.

1. Two-out-of-four NSSS ESFAS steam generator low-low signals (two-out-of-three steam generators)

2. 4.16 kV bus low voltage from two-out-of-four channels with the diesel generator breaker closed.

3. ATWS Mitigation System initiation signals.

216 | Two separate and redundant actuation trains are initiated by the signal (see table 7.3-3, item 6). The ESP does not have the capability to initiate the auxiliary feedwater signal - turbine-driven; however, control of the auxiliary feedwater system is accomplished from the ESP by individual actuation of the equipment. A detailed list of equipment activated by the AFS-TD is shown on table 7.3-19, item 6.

This design of the automatic initiation of the auxiliary feedwater system complies with Section II.E.1.2 of NUREG-0660.

G. Diesel Generator Load Sequencer Signals (SEQ)
The diesel generator load sequencer signals are automatically initiated by receipt of safety injection signals from the NSSS ESFAS (LOCA segment) and/or by an undervoltage signal from the 4.16 kV Class 1E bus loss of voltage (LOV) segment.

The following types of diesel generator load sequencer signals are generated to control ESF equipment:

1. Type A = SIS. or SIS coincident with LOV
2. Type B = SIS. or LOV. or SIS coincident with LOV
3. Type C = LOV

   Refer to figure 7.3-4.

The diesel generator load sequencer provides safety-related controls for ESF equipment during the following plant accident conditions:

a. Loss-of-Coolant Accident (LOCA)

   The diesel generator load sequencer is automatically initiated by the receipt of SIS signals. The Class 1E equipment already operating continues to operate and the diesel generator load sequencer starts the diesel engine and generates Type A and B signals to start any additional required ESF equipment in programmed time sequence.

   Refer to figure 7.3-4.

b. Loss of Voltage (LOV) to the 4.16 kV Class 1E Bus

   The diesel generator load sequencer is automatically initiated by receipt of a two-out-of-four undervoltage signal at the 4.16 kV Class 1E bus to which the diesel generator is connected. The diesel generator load sequencer starts the diesel engine. sheds all the loads connected to the Class 1E bust trips and locks out both offsite power feeder breakers. and generates a permissive signal to close the diesel generator breaker. When the diesel generator reaches rated voltage and frequency. the diesel generator breaker closes and the diesel generator load sequencer generates Type B and C signals to start ESF equipment in programmed time sequence.

The diesel generator is able to accept loads within 10 seconds after receipt of a LOV signal: all ESF equipment is connected to the Class 1E bus within 60 seconds of the Class 1E bus energization.

c. LOCA followed by LOV

If during a LOCA load sequence segment a LOV signal is generated, the diesel generator load sequencer will immediately reset all Type A and B signals, shed all loads connected to the Class 1E bus, trip the offsite power supply feeder breakers, and generate a permissive signal to close the diesel generator breaker. When the diesel generator reaches nominal voltage and frequency, the diesel generator breaker will close and the load sequencer will reinitiate Type A and B signals to start ESF equipment in programmed time sequence.

d. LOV followed by LOCA

If SIS signals are generated during the LOV load sequencer segment, the diesel generator load sequencer will immediately reset all Type B and C signals and will reinitiate Type A and B signals to start ESF equipment in the programmed time sequence.

7.3.1.1.5 Analog Circuitry

7.3.1.1.5.1 NSSS Analog Circuitry. The process analog sensors and racks for the NSSS ESFAS are covered in reference 1. Discussed in this report are the parameters to be measured, including pressures, tank and vessel water levels, and temperatures, as well as the measurement and signal transmission considerations. Other considerations covered are automatic calculations, signal conditioning, and location and mounting of the devices.

The sensors monitoring the primary system are located as shown on the piping flow diagrams in chapter 5. The secondary system sensor locations are shown on the steam system piping and instrumentation drawings given in chapter 10.

The sensors are arranged as shown on figure 7.3-10.

There are four instrument lines that penetrate the containment and that are required to remain functional following a LOCA or steam line break inside containment. These lines sense the pressure of containment atmosphere on the inside and are connected to pressure transmitters on the outside. Signals from these transmitters can initiate safety injection and containment isolation on Hi-1 containment pressure, and initiate main steam line isolation on Hi-2 containment pressure. These signals also, upon Hi-3 containment pressure, produce the automatic signal to initiate containment spray and provide post-accident monitoring of containment pressure. In view of these functions, these lines do not have automatic isolation valves, since it is essential that the lines remain open and not be isolated following an accident. Based on this requirement, a sealed sensing line as described below is used.

The containment pressure sensing lines are connected to containment atmosphere by a filled and sealed hydraulic transmission system. This arrangement, together with the pressure transmitters external to the containment, forms a double barrier and complies with Regulatory Guide 1.11: Should a leak occur in any sensing line outside containment, the sealed bellows inside containment will prevent the escape of containment atmosphere. Since each of the sealed bellows is designed to withstand full containment pressure, should a leak occur in any sensing line inside containment, the diaphragm in the transmitter will prevent any escape from containment. This arrangement provides automatic double barrier isolation without operator action, and without sacrificing any reliability with regard to its safeguards functions (i.e., no valves to be inadvertently closed). Both the bellows and tubing inside containment and the transmitter and tubing outside containment are enclosed by protective shielding. Because of this sealed fluid-filled bellows system, a postulated severance of the line during either normal operation or accident conditions will not result in any releases from the containment.

7.3.1.1.5.2 BOP Analog Circuitry. The process analog sensors for the BOP ESFAS are arranged as shown in figure 7.3-11.

7.3.1.1.6 Digital Circuitry

7.3.1.1.6.1 NSSS Digital Circuitry. The NSSS ESF logic racks are discussed in detail in reference 2. The description includes the considerations and provisions for physical and electrical separation as well as details of the circuitry. Reference 2 also covers certain aspects of online test provisions, provisions for test points, considerations for the

instrument power source, and considerations for accomplishing physical separation. The outputs from the analog channels are combined into actuation logic as shown on sheets 5 (Tavg), 6 (pressurizer pressure), 7 (low steam line pressure), 8 (ESF actuation), 15 (auxiliary feedwater) of figure 7.2-1. To facilitate ESF actuation testing, four cabinets (two per train) are provided that enable operation, to the maximum practical extent, of safety features loads on a group by group basis until actuation of all devices has been checked (see reference 3). Final actuation testing is discussed in detail in subsection 7.3.2.

7.3.1.1.6.2 BOP Digital Circuitry. The logic of BOP ESFAS circuitry is made up of solid-state components with electro-mechanical relays that function as isolators for signals to the station annunciator and computer.

Trip bistables in the sensing channels monitor the radio-activity signals and feed continuous electrical (fail-safe) signals into one-out-of-two coincident matrices. Should any of the variables exceed their trip set points, the bistables trip and cease sending output signals. Should one of the two bistables monitoring the same variable cease to send output signals, the normally energized output relays initiate the actuation signal to the actuated equipment.

Two trains of actuation signals are derived from the two sensing channels. Memory is provided in the trip bistables and in the actuation output circuit. Both must be manually reset.

7.3.1.1.7 Final Actuation Circuitry

7.3.1.1.7.1 NSSS Final Actuation Circuitry. The outputs of the solid-state protection system (SSPS) (the slave relays) are energized to actuate, as are most final actuators and actuated devices of the ESF. Certain SSPS slave relay contacts are connected as inputs to the Solid-State Interposing Logic System (SSILS) which is part of the BOP. Thus, final actuators are controlled by the SSILS output relays, so that one SSPS slave relay may operate several final actuators. A detail of the final equipment actuated by the NSSS ESF signals is shown on table 7.3-18.

7.3.1.1.7.2 BOP Final Actuation Circuitry. The outputs of the solid-state interposing logic system (SSILS) (output relays) are energized-to actuate, as are most final actuators and actuated devices of the ESF. A detail of final actuated equipment by the BOP ESF signals is shown on table 7.3-19.

7.3.1.1.8 Support Systems

The following systems are provided in support of the ESF:

A. Nuclear service cooling water system (see subsection 9.2.1)

B. Component cooling water systems (see subsection 9.2.2)

C. Electrical power distribution system (see chapter 8)

D. Safety-related heating, ventilating, and air conditioning (HVAC) support systems (see chapter 9)

E. Safety-related instrument air system (see subsection 9.3.1).

7.3.1.2 Design Bases Information

The functional diagrams presented in figure 7.2-1, sheets 5, 6, 7, and 8, provide a graphic outline of the functional logic associated with requirements for the NSSS ESFAS.

Requirements for the ESF system are given in chapter 6. Given below is the design bases information required in IEEE Standard 279.[4]

7.3.1.2.1 Generating Station Conditions

The following is a summary of those generating station conditions requiring protective action:

A. Primary system:

1. Rupture in small pipes or cracks in large pipes
2. Rupture of a reactor coolant pipe (LOCA)
3. Steam generator tube rupture.

B. Secondary system:

1. Minor secondary system pipe breaks resulting in steam release rates equivalent to a single dump, relief, or safety valve
2. Rupture of a major steam pipe.

7.3.1.2.2 Generating Station Variables

Tables 7.3-4 and 7.3-5 summarize the generating station variables required to be monitored for the automatic initiation of ESF during each accident identified in the preceding paragraph. Post-accident monitoring system indicators available to the operators are given on table 7.5-1.

7.3.1.2.3 Spatially Dependent Variables

Of the variables sensed by the ESFAS, only reactor coolant temperature requires particular consideration and special measurement techniques to account for spatial dependence. The spatial effects phenomenon is negated by taking multiple samples (three) from the reactor coolant hot leg and averaging these samples by mixing in the RTD bypass loop.

7.3.1.2.4 Limits, Margins, and Levels

Prudent operational limits, available margins, and set points before onset of unsafe conditions requiring protective action
946| are discussed in chapters 15 and ITS Chapter 1.

7.3.1.2.5 Abnormal Events

The malfunctions, accidents, or other unusual events which are considered in the design of protection system components are as follows:

A. Loss-of-coolant accident (see section 15.6)

B. Secondary system accidents (see section 15.1)

C. Earthquakes (see chapters 2 and 3)

D. Fire (see subsection 9.5.1)

E. Explosion (hydrogen buildup inside containment) (see subsection 6.2.5)

F. Missiles (see section 3.5)

G. Flood (see sections 2.4 and 3.4).

7.3.1.2.6 Minimum Performance Requirements

The ESFAS response time is defined as the interval required for the ESF sequence to be initiated subsequent to the time that

the appropriate variable(s) exceed the set point(s). The ESF sequence is initiated by the output of the ESFAS which is by the operation of the dry contacts of the slave relays (600 and 700 series relays) in the output cabinets of the solid-state protection system (SSPS). The response times listed in tables 7.3-4 and 7.3-5 include the interval of time that will elapse between the time the parameter, as sensed by the sensor, exceeds the safety set point and the time the SSPS slave relay dry contacts are operated. These values, listed in tables 7.3-4 and 7.3-5, are maximum allowable values consistent with the safety analysis and the technical specifications and are systematically verified during plant preoperational startup tests. For the overall ESF response time, refer to ITS Chapter 1 Table 3.3.2-2 of the technical specifications. |848
For the overall reactor trip system instrumentation response time, refer to ITS Chapter 1 Table 3.3.1-2 of the technical specifications. |848

7.3.1.3 Final System Drawings

The schematic diagram for the systems discussed in this section is listed in section 1.7.

7.3.2 ANALYSIS

7.3.2.1 Failure Mode and Effects Analysis

Failure mode and effects analyses (FMEA) have been performed on ESF systems equipment within the Westinghouse scope of supply as stated in reference 7. The results verify that these systems meet protection single failure criteria as required by IEEE Standard 279.

For BOP safety systems, the assurance that safety-related instrumentation and control fulfill their functions (assuming a single failure) is achieved by the use of redundant channels, trains, components, and power supplies with the appropriate separation provided between them. Detailed documentation in the form of FMEAs tables are provided in each respective subsection.

7.3.2.2 Compliance with Standards and Design Criteria

Discussion of the General Design Criteria (GDC) is provided in various sections of chapter 7 where a particular GDC is applicable. Applicable GDCs include Criteria 11, 13, 20, 21, 22, 23, 24, 25, 26, 27, 28, 35, 37, 38, 40, 43, and 46. Compliance with certain IEEE Standards and USNRC Regulatory Guides is presented in subsection 7.1.2. The discussion given below shows that the ESFAS complies with IEEE Standard 279.

L3.2.2.1 Single Failure Criteria

The discussion presented in subparagraph 7.2.2.2.3 is applicable to the ESFAS, with the following exception: In the ESF, a loss of instrument power will call for actuation of ESF equipment controlled by the specific bistable that lost power (containment spray excepted). The actuation equipment must have power to comply (main steam and auxiliary feedwater isolation are excepted). The power supply for the protection systems is discussed in section 7.6 and in chapter 8.

For containment spray, the final bistables are energized to trip to avoid spurious actuation. In addition, manual containment depressurization requires a simultaneous actuation of two manual controls. This is considered acceptable because containment spray actuation on Hi-3 containment pressure signal provides automatic initiation of the containment spray system via protection channels meeting the criteria in IEEE Standard 275. Moreover, two sets (two switches per set) of containment spray manual initiation switches are provided to meet the requirements of IEEE Standard 279. Also, it is possible for all ESF equipment (valves, pumps, etc.) to be individually, manually actuated from the control board. Hence, a third mode of containment spray initiation is available. The design meets the requirements of General Design Criteria 21 and 23 of 10 CFR 50, Appendix A.

7.3.2.2.2 Equipment Qualification

The subject of equipment qualification is discussed in sections 3.10 and 3.11.

7.3.2.2.3. Channel Independence

A. NSSS Channel Independence

2

The discussion presented in subparagraph 7.2.2.2.3.6 is applicable. The ESF slave relay outputs from the solid-state logic protection cabinets are redundant. The actuations associated with each train are energized up to and including the final actuation devices by the separate ac power supplies that power the logic trains. An exception is the main feedwater pump turbine trip initiated by steam generator high-high level and SIS.

An isolation relay is utilized in the design to isolate the Class 1E portion from the non-Class 1E portion of the signal. In addition, physical separation of the raceways is provided from the sensor to the actuation device.

B. BOP Channel Independence

The BOP SSILS cabinets and radiation monitor cabinets have been designed in accordance with Regulatory Guide 1.75. The ESF output relays from the SSILS are redundant and the actuations associated with each train are energized up to and including the final actuators by the separate ac power supplies that power the logic trains.

The system is composed of the redundant Trains A and B. The instrumentation and controls of the components and equipment in Train A are physically and electrically separate, and independent of the instrumentation and controls of the components and equipment in Train B. The redundancy and independence provided between safety Trains A and B are adequate to maintain equipment functional capabilities following design basis events.

Pumps and valves that are an integral part of, or associated with, the engineered safeguards will have an operation/position status light.

ESF remote-operated valves have position indication on the control board to show proper positioning of the valves. Red and green indicator lights are an integral part of manual control station showing open and closed positions. The ESF position of equipment is displayed by an energized light on the status light panels, which consist of an array of white lights that are off when the equipment is in its normal or required position for power operations. These status lights thus enable the operator to quickly assess the status of the ESF systems. These indications are derived from contacts integral to the valve operators. The circuits for the ESF status lights are classified as nonsafety-related.

7.3.2.2.4 Control and Protection System Interaction

The discussions presented in subparagraph 7.2.2.2.3 are applicable.

7.3.2.2.5 NSSS Capability for Sensor Checks and Equipment Test and Calibration

The discussion of system testability in subparagraph 7.2.2.2.3 is applicable to the sensors, analog circuitry, and logic trains of the NSSS ESFAS.

The following discussions cover those areas in which the testing provisions differ from those for the reactor trip system:

7.3.2.2.5.1 Testing of Engineered Safety Features Actuation Systems. The ESFAS are tested to provide assurance that the systems will operate as designed, and will be available to function properly in the unlikely event of an accident. Typical ESF test cabinets are discussed in reference 3, which is furnished for information only and is not intended to necessarily reflect the as-designed testing for this plant. The testing program agrees with GDC 21, 37, 40, and 43 and Regulatory Guide 1.22 as discussed in paragraph 7.1.2.5. The tests described herein and further discussed in subsection 6.3.4. meet the requirements on testing of the ECCS as stated in GDC 37, except for the operation of those components that will cause an actual safety injection. The test, as described, demonstrates the performance of the full operational sequence that brings the system into operation, the transfer between normal and emergency power sources, and the operation of associated cooling water systems. The charging pumps and residual heat removal pumps are started and operated, and their performance verified in a separate test discussed in subsection 6.3.4. When the pump tests are considered in conjunction with the ECCS test, the requirements of GDC 37 on testing of the ECCS are met as closely as possible without causing an actual safety injection.

Testing as described in section 6.3 and in subparagraphs 7.2.2.2.3 and 7.3.2.2.5 provides complete periodic testability during reactor operation of all logic and components associated with the ECCS. This design agrees with Regulatory Guide 1.22 as discussed in the above sections. The program is as follows:

A. Prior to initial plant operations, ESFAS tests will be conducted.

B. Subsequent to initial startup, ESFAS tests will be conducted during each regularly scheduled refueling outage.

C. During online operation of the reactor, all of the ESF analog and logic circuitry will be fully tested. In addition, essentially all of the ESF final actuators will be fully tested. The remaining few final actuators, whose operation is not compatible with continued on-line plant operation, will be checked by means of continuity testing (see paragraph 7.1.2.5).

7.3.2.2.5.2 Performance Test Acceptability Standard for the Safety Injection Signal and for the Automatic Signal for Containment Spray Actuation Generation. During reactor operation, the basis for ESFAS acceptability will be successful completion of the overlapping tests performed on the initiating system and the ESFAS (see figure 7.3-2, sheet 1). Checks of process indications verify operability of the sensors. Analog checks and tests verify the operability of the sensors. Analog checks and tests verify the operability of the analog circuitry from the input of these circuits through to, and including, the logic input relays, except for the input relays associated with the containment spray functions that are tested during the solid-state logic testing. Solid-state logic testing also checks the digital signal path from, and including logic input relay contacts through, the logic matrices and master relays, and performs continuity tests on the coils of the output slave relays. Final actuator testing operates the output slave relays and verifies operability of those devices that require safeguards actuation and that can be tested without causing plant upset. A continuity check is performed on the actuators of the untestable devices. Operation of the final devices is confirmed by control board indication and visual observation that the appropriate pump breakers close and automatic valves shall have completed their travel.

The basis for acceptability for the ESF interlocks will be control board indication of proper receipt of the signal upon introducing the required input at the appropriate set point.

Maintenance checks (performed during regularly scheduled refueling outages), such as resistance-to-ground of signal cables in radiation environments, are based on qualification test data that identifies what constitutes acceptable radiation, thermal, etc., degradation.

7.3.2.2.5.3 Frequency of Performance of Engineered Safety Features Actuation Tests. During reactor operation, complete system testing (excluding sensors or those devices whose operation would cause plant upset) is performed in accordance with the technical specifications as specified in ITS Chapter 1. Testing, including the sensors, is also performed during scheduled plant shutdown for refueling. |648

7.3.2.2.5.4 Engineered Safety Features Actuation Test Description. The following paragraphs describe the testing circuitry and procedures for online portions of the testing program. The guidelines used in developing the circuitry and procedures are:

A. The test procedures must not involve the potential for damage to any plant equipment.

B. The test procedures must minimize the potential for accidental tripping of plant systems.

C. The provisions for online testing must minimize complication of ESF actuation circuits so that their reliability is not degraded.

7.3.2.2.5.5 Description of Initiation Circuitry. Several systems (as listed in subparagraph 7.3.1.1.1) comprise the total ESFAS, the majority of which may be initiated by different process conditions, and may be reset independently of each other.

The remaining functions (listed in subparagraph 7.3.1.1.1) are initiated by a common signal (safety injection signal) which, in turn, may be generated by different process conditions.

In addition, operation of other vital auxiliary support systems, such as auxiliary feedwater, is initiated by the safety injection signal.

Each function is actuated by a logic circuit that is available from either of the two redundant trains of ESF initiation circuits.

The output of each of the initiation circuits consists of a master relay that drives slave relays for contact multiplication as required. The master and slave relays are mounted in the ESFAS cabinets, designated Train A and Train B, respectively, for the redundant counterparts. The master and slave relay circuits in most cases operate various pump and fan circuit breakers or starters, motor-operated valve contactors, solenoid-operated valves, emergency diesel generator starting, etc., through the SSILS.

7.3.2.2.5.6 Analog Testing. Analog testing is identical (except as noted) to that used for reactor trip circuitry and is described in section 7.2.

An exception to this is containment spray, which is energized to actuate 2/4 and reverts to 2/3 when one channel is in test.

7.3.2.2.5.7 Solid-State Logic Testing. Except for containment spray actuation channels, solid-state logic testing is the same as that discussed in section 7.2. During logic testing of one train, the other train can initiate the required ESF function. For additional details, see reference 2.

7.3.2.2.5.8 Actuator Testing. Using the method discussed in section 7.2. testing of the initiation circuits through operation of the master relay and its contacts to the coils of the slave relays as been accomplished. Slave relays do not operate because of reduced voltage.

The ESF system final actuation device or actuated equipment testing shall be performed from the ESF test cabinets. These cabinets are normally located near the solid-state protection system equipment. There is one set of test cabinets provided for each of the two protection Trains A and B. Each set of cabinets contains individual test switches necessary to actuate the slave relays. To prevent accidental actuation, test switches are of the type that must be rotated and then depressed to operate the slave relays. Assignments of contacts of the slave relays for actuation of various final devices or actuators has been made such that groups of devices, or actuated equipment, can be operated individually during plant operation without causing plant upset or equipment damage. In the unlikely event that a safety injection signal is initiated during the test of the final device that is actuated by this test, the device will already be in its position.

During this last procedure, close communication between the main control room operator and the operator at the test panel is required. Prior to the energizing of a slave relay, the operator in the main control room assures that plant conditions will permit operation of the equipment that will be actuated by the relay.

After the tester has energized the slave relay, the main control room operator observes that all equipment has operated as indicated by appropriate indicating lamps, monitor lamps, and annunciators on the control board and, using a prepared checklist, records all operations. He then resets all devices and prepares for operation of the next slave relay-actuated equipment.

By means of the procedure outlined above, all ESF devices actuated by ESFAS initiation circuits, with the exceptions noted in paragraph 7.1.2.5 under a discussion of Regulatory Guide 1.22, are operated by the automatic circuitry.

7.3.2.2.5.9 Actuator Blocking and Continuity Test Circuits. Those few final actuation devices that cannot be designed to be actuated during plant operation (discussed in paragraph 7.1.2.5) have been assigned to slave relays for which additional test circuitry has been provided to individually block actuation of a final device upon operation of the associated slave relay during testing. Operation of these slave relays, including

contact operation, and continuity of the electrical circuits associated with the final (in some cases interposing) devices control are checked in lieu of actual operation. The circuits provide for monitoring of the slave relay contacts in some cases, or the SSILS output relays in most cases, the devices control circuit cabling, control voltage and the devices actuation solenoids. Interlocking prevents blocking the output from more han one output relay in a protection train at a time. Interlocking between trains is also provided to prevent continuity testing in both trains simultaneously: therefore, the redundant device associated with the protection train not under test will be available in the event protection action is required. If an accident occurs during testing, the automatic actuation circuitry will override testing as noted above. One exception to this is that if the accident occurs while testing a slave relay whose output must be blocked, those few final actuation devices associated with this slave relay will not be overridden: however, the redundant devices in the other train would be operational and would perform the required safety function. Actuation devices to be blocked are identified in paragraph 7.1.2.5.

The continuity test circuits for these components that cannot be actuated online are verified by proving lights on the ESF test racks.

The typical schemes for blocking operation of selected protection function actuator circuits are shown in figure 7.3-2, sheet 2 as details A and B. The schemes operate as explained below and are duplicated for each ESF train.

Detail A shows the circuit for contact closure for protection function actuation. Under normal plant operation, and equipment not under test, the lamps "DS*" for the various circuits will be energized. Typical circuit path will be through the normally close test relay contact "KΘ*" and through test lamp connection 1 to 3. Coil "X2" and "X3" will be capable of being energized for protection function actuation upon closure of solid-state logic output relay contacts "K*". Coil "X2" and "X3" is typical for a breaker closing auxiliary coil, motor starter master coil, coil of a solenoid valve, auxiliary relay, etc. When the contacts "KΘ*" are opened to block energizing of coil "X2" and "X3", the white lamp is de-energized and the slave relay "K*" may be energized to perform continuity testing. This continuity testing is verified by depressing test lamp "DS*" and observing that the lamp lights through connection 2 and 1 (contact "KΘ*" open) through solid-state interposing logic output relay contact (now closed) and finally through actuator coil "X2" and "X3". Sufficient current will flow in the circuit to cause the lamp to glow but insufficient to cause the actuator coil "X2" and "X3" to operate. To verify operability of the blocking relay

in both blocking and restoring normal service, open the blocking relay contact in series with lamp connections and the test lamp should be de-energized: close the blocking relay contact in series with the lamp connections and the test lamp should now be energized, which verifies that the circuit is now in its "normal" condition, i.e., operable.

Detail B shows the circuit for contact opening for protection function actuation. Under normal plant operation, and equipment not under test, the white test lamps "DS*" for the various circuits will be energized, and green test lamp "DS*" will be de-energized. Typical circuit path for white lamp "DS*" will be through the normally closed solid-state logic output relay contact "K*" and through test lamp connections 1 to 3. Coils "Y1" and "Y2" will be capable of being de-energized for protection function actuation upon opening of solid-state logic output relay contacts "K*". Coil "Y2" is typical for a solenoid valve coil, auxiliary relay, etc. When the contacts "K0*" are closed to block de-energizing of coils "Y2", the green test lamp is energized, and the slave relay "K*" may be energized to verify operation (opening of its contacts). To verify operability of the blocking relay in both blocking and restoring normal service, close the blocking relay contact to the green lamp: the green test lamp should now be energized. Open this blocking relay contact: the green test lamp should be de-energized, which verifies that the circuit is now in its "normal", i.e., operable position.

7.3.2.2.5.10 Time Required for Testing. It is estimated that analog testing can be performed at a rate of several channels per hour. Logic testing of Trains A and B can be performed in less than 30 minutes. Testing of actuated components (including those that can only be partially tested) will be a function of control room operator availability. It is expected to require several shifts to accomplish these tests. During this procedure, automatic actuation circuitry will override testing, except for those few devices associated with a single slave relay whose outputs must be blocked and then only while blocked. It is anticipated that continuity testing associated with a blocked slave relay could take several minutes. During this time the redundant devices in the other trains would be operable.

7.3.2.2.5.11 Summary of Online Testing Capabilities. The procedures described provide capability for checking completely from the process signal to the logic cabinets, and from there to the individual pump and fan circuits breakers or starters, valve contactors, pilot solenoid valves, etc., including all field cabling actually used in the circuitry called upon to

operate for an accident condition. For those few devices whose operation could adversely affect plant or equipment operation, the same procedure provides for checking from the process signal to the logic rack. To check the final actuation device, a continuity test of the individual control circuits is performed.

The procedures require testing at various locations:

A. Analog testing and verification of bistable set points are accomplished at process analog racks. Verification of bistable relay operation is done at the main control room status lights.

B. Logic testing through operation of the master relays and low voltage application to slave relays is done at the logic rack test panel.

C. Testing of pumps, fans, and valves is done at a test panel located in the vicinity of the logic racks in combination with the control room operator.

D. Continuity testing for those circuits that cannot be operated is done at the same test panel mentioned in C above.

The reactor coolant pump's essential service isolation valves consist of the isolation valves for the component cooling water and the seal water return header. The main reason for not testing these valves periodically is that the reactor coolant pumps may be damaged. Although pump damage from this type of test would not result in a situation that endangers the health and safety of the public, it could result in unnecessary shut-down of the reactor for an extended period of time until the reactor coolant pump or certain of its parts could be replaced.

Containment spray system tests will be performed periodically. The pump tests will be performed with the isolation valves in the spray supply lines at the containment and spray chemical additive tank closed. The valve tests are performed with the pumps stopped. During this testing, automatic actuation circuitry will override testing.

7.3.2.2.5.12 Testing During Shutdown. The ECCS tests will be performed at each major fuel reloading with the RCS isolated from the ECCS by closing the appropriate valves. A test safety injection signal will then be applied to initiate operation of active components (pumps and valves) of the ECCS. This is in compliance with GDC 37 of 10 CFR 50, Appendix A.

7.3.2.2.5.13 Periodic Maintenance Inspections. The maintenance procedures that follow may be accomplished in any order. The frequency will depend on the operating conditions and requirements of the reactor power plant. If any degradation of equipment operation is noted, either mechanically or electrically, remedial action is taken to repair, replace, or readjust the equipment. Optimum operating performance must be achieved at all times.

Typical maintenance procedures include the following:

A. Check cleanliness of all exterior and interior surfaces.

B. Cheak all fuses for corrosion.

C. Inspect for loose or broken control knobs and burned out indicator lamps.

D. Inspect for moisture and condition of cables and wiring.

E. Mechanically check all connectors and terminal boards for looseness, poor connection, or corrosion.

F. Inspect the components of each assembly for signs of overheating or component deterioration.

G. Perform complete system operating check.

The balance of the requirements listed in IEEE Standard 279 (paragraphs 4.11 through 4.22) is discussed in section 7.2. Paragraph 4.20 receives special attention in section 7.5.

7.3.2.2.6 NSSS Manual Resets and Blocking Features

The manual reset feature associated with containment spray actuation is provided in the standard design of the solid-state protection system design for two basic purposes. First, the feature permits the operator to start an interruption procedure of automatic containment spray in the event of false initiation of an actuate signal. Second, although the system performance is automatic, the reset feature enables the operator to start a manual takeover of the system to handle unexpected events that can be better dealt with by operator appraisal of changing conditions following an accident.

It is most important to note that manual control of the system does not occur once actuation has begun by just resetting the

associated logic devices alone. Components will seal in (latch) so that removal of the actuate signal, in itself, will neither cancel nor prevent completion of protective action, nor provide the operator with manual override of the automatic system by this single action. In order to take complete control of the system to interrupt its automatic performance, the operator must deliberately remove the initial actuate signals, in addition to tripping the pump motor circuit breakers, if stopping the pumps is desirable or necessary.

The feature of manual reset associated with containment spray (phase B containment isolation) as well as with phase A containment isolation and control room isolation, does not perform a bypass function. It is merely the first of several manual operations required to take control from the automatic system or interrupt its completion should such an action be considered necessary.

In the event that the operator anticipates system actuation, and erroneously concludes that it is undesirable or unnecessary, and imposes a standing reset condition in one train (by operating and holding the corresponding reset switch at the time the initiate signal is transmitted), the other train will automatically carry the protective action to completion. In the event that the reset condition is imposed simultaneously in both trains at the time the initiate signals are generated, the automatic sequential completion of system action is interrupted and control has been taken by the operator. Manual takeover will be maintained, even though the reset switches are released, if the original initiate signal exists. Should the initiate signal then clear and return again, automatic system actuation will repeat.

Note also that any time delays imposed on the system action are to be applied after the initiating signals are latched.

The manual block features associated with pressurizer and steam line safety injection signals provide the operator with the means to block initiation of safety injection during plant startup. These block features meet the requirements of Paragraph 4.12 of IEEE Standard 279 in that automatic removal of the block occurs when plant conditions require the protection system to be functional.

7.3.2.2.7 NSSS Manual Initiation of Protective Actions (Regulatory Guide 1.62)

The NSSS ESFAS agrees with Regulatory Guide 1.62 with the following clarification:

A. With regard to Regulatory Position C-1:

1. Manual initiation at the system level is interpreted to mean no more than three operator actions resulting in at least one train, division, or channel of final actuation devices including support systems, except for the additional clarification involving safety injection to cold leg recirculation (and cold leg to hot leg) switchover as described in section 6.3 and below.

2. Engineering judgment will be exercised to assure that a minimum of operator actions are required to achieve system level manual initiation without unnecessarily jeopardizing the return to operation of the power plant.

3. Designs requiring more than two operator actions per train, division, or channel to achieve protective action are to be limited to those actions that are required following the first few minutes of the accident and that will be evaluated on a case basis.

B. With regard to Regulatory Position C-2:

All equipment that contributes to the protective action will be initiated at the system level.

C. With regard to Regulatory Position C-3:

Switches for manual initiation will be located in the control room in such a manner as to permit deliberate expeditious action by the operator.

D. With regard to Regulatory Position C-4 and Paragraph 4.17 of IEEE Standard 279:

1. Equipment common to both manual and automatic initiation will be minimized. Where manual and automatic action sequencing functions and interlocks that contribute to the protective action are common, component or channel level initiation will also be provided in the control room.

2. Manual initiation portions of the protection system will meet the single failure criteria.

3. Manual initiation portions of the protection system will not impair the ability of the automatic system to meet the single failure criteria.

4. No exception to the requirements of IEEE Standard 279 has been taken in the manual initiation circuit of safety injection. Although Paragraph 4.17 of IEEE Standard 279 requires that a single failure within common portions of the protective system shall not defeat the protective action by manual or automatic means, the standard does not specifically preclude the sharing of initiated circuitry logic between automatic and manual functions. It is true that the manual safety injection initiates functions associated with one actuation train (e.g., Train A) shares portions of the automatic initiation circuitry logic of the same logic train: however, a single failure in shared functions does not defeat the protective action of the redundant actuation train (e.g., Train B). A single failure in shared function does not defeat the protective action of the safety function. It is further noted that the sharing of the logic by manual and automatic initiation is consistent with the system level action requirements of the IEEE Standard 279, Paragraph 4.17, and is consistent with minimization of complexity.

E. With regard to Regulatory Position C-6:

Manual initiation portions of the protection system are designed so that once initiated, a protection action at the system level (initiation of the final actuation device associated with a given protective function) goes to completion.

Having gone to completion: (i.e., once sufficient breakers are closed or sufficient MOVs or other actuation are operated), the system is designed to require at least two operator actions to return actuated equipment to pre-initiation status.

This design is in compliance with the applicable section of IEEE Standard 279 (Paragraph 4.16).

F. In addition, manual initiation is provided to allow the operator to take early action based on observation of plant parameters. It is not to be treated as a backup to automatic features. Operator actions will not be required to satisfy the single failure criteria.

G. When only one channel, division, or train is assigned to a single control device, this creates less complexity in switch design, although it will require the operator to initiate redundant functions using separate controls.

There are three individual main steam stop valve momentary control switches (one per loop) mounted on the control board. Each switch, when actuated, will isolate one of the main steam lines. In addition, there will be two system level switches, either switch actuating'all main steam lines at the system level.

Manual initiation of semi-automatic switchover to recirculation following a loss-of-primary-coolant accident is in compliance with Paragraph 4.17 of IEEE Standard 279, with the following comments:

A. The manual operations that are involved in this switchover are described in section 6.3.

B. Once safety injection is initiated following a loss-of-primary-coolant accident, the containment sump isolation valves in the RHR system pump suction lines will open automatically upon receipt of a low-low level signal from the RWST level instrumentation.

C. Manual initiation of either one or two redundant safety injection actuation main control board-mounted switches not only provides for actuation of the components required for reactor protection and mitigation of adverse consequences of the postulated accident prior to the recirculation mode associated with a loss-of-primary-coolant accident, but also enables the containment sump isolation valves to automatically open when the low-low level set point on the RWST is reached. Manual operation of other components or manual verification of proper position as part of emergency procedures is not precluded nor otherwise in conflict with the above described compliance to Paragraph 4.17 of IEEE Standard 279 of the semi-automatic switchover circuits. Although manual actuation of main steamline isolation (all valves), containment isolation (phase A), and containment spray acturation is not within the NSSS

scope. the same criteria herein described for the manual safety injection also applies to these aforementioned manual actuation functions in the BOP scope.

7.3.3 BOP CONSIDERATIONS

The following considerations are provided for the BOP systems.

7.3.3.1 Instrument Air System

A loss of reactor plant normal instrument air (assuming no other accident conditions) cannot cause safety limits, as given in
440| ITS Chapter 1, to be exceeded. Likewise, the loss will not adversely affect the core or the RCS, nor will it prevent an orderly shutdown if this is necessary. It is noted that, for conservatism during the accident analysis (chapter 15), credit is not taken for the instrument air system nor for any control system benefit. A safety-related instrument air system is provided as described in subsection 9.3.1

7.3.3.2 Auxiliary Feedwater System

7.3.3.2.1 Description

The system consists of two motor-driven pumps, and one steam turbine-driven pump, associated piping, valves, instruments, and controls as shown in figure 10.4-9. The two motor-driven pumps and the turbine-driven pump are started automatically by signals from the automatic start logic as shown in figure 7.3-3. All three pumps can also be started manually from control switches in the control room, and at the emergency shutdown panel.

Each motor-driven pump feeds all three steam generators through individual, normally modulating air-operated, flow control valves that fail in the open position in the event of a loss of instrument air or in the modulating position in the event of a loss of both sources of Class 1E power to the solenoid valves. Auxiliary feedwater flow can be regulated manually from the control room or the emergency shutdown panel.

The turbine-driven pump feeds all three steam generators through individual, normally modulating air-operated, flow control valves that fail in the open position in the event of a loss of instrument air or in the modulating position in the event of a loss of both Class 1E powers to the solenoid valves. Auxiliary feedwater flow can be regulated manually from the control room or the emergency shutdown panel.

Each turbine-driven pumps flow control valve is supplied with a backup air accumulator with sufficient capacity to permit remote valve closure from the control room or from the emergency shutdown panel. Local manual valve operation by a handwheel is also available.

Each motor-driven pumps flow control valve is connected to the safety-related grade instrument air system to permit remote valve operation from the control room or from the emergency shutdown panel for post-accident operation for a period of time sufficient to bring the plant to a cold shutdown condition. Local manual valve operation by a handwheel is also available.

Redundant, safety-related auxiliary feedwater flow indication is provided for each steam generator in the control room and at the emergency shutdown panel.

This design complies with Section II.E.1.2 of NUREG-0660.

The auxiliary feedwater pump turbine is supplied with motive power from two main steam lines through a normally closed pneumatic operated steam to auxiliary feedwater pump (AFP) turbine isolation valve and a normally open motor-operated trip and throttle valve. A hydraulic-operated, turbine governor valve is also provided at the inlet to the pump driver. Control of the steam supply and turbine stop valves for the turbine-driven pump is provided in the control room and at the emergency shutdown panel.

The status of the motor-driven pumps and auxiliary feedwater flow control valves are indicated in the control room and at the emergency shutdown panel. The status of turbine-driven pumps and turbine trip and throttle valve are indicated in the control room, as well as at auxiliary feedwater turbine local panel.

The auxiliary feedwater system equipment is described in subsection 10.4.9.

7.3.3.2.1.1 System Description

A. Initiating circuit

The motor-driven pumps are initiated automatically by the (BOP ESFAS) AFS-MD signals (these signals also close the blowdown isolation and sample line valves for all steam generators).

The turbine-driven pump is initiated automatically by the (BOP ESFAS) AFS-TD.

The automatic initiating signals and circuits are designed so that their failure will not preclude manual initiation of the auxiliary feedwater system from the control room. Likewise, the manual initiation circuits are designed such that a single failure will not result in loss of system function.

All initiating signal circuitry required to ensure that auxiliary feedwater system performs its safety functions are powered from emergency power buses.

B. Logic

See figure 7.3-3 for auxiliary feedwater system control logic information.

C. Bypass

Indication of system bypass is as described in section 7.5.

D. Interlocks

There are no interlocks in the auxiliary feedwater system.

E. Redundancy

Sufficient actuation and control channels are provided throughout the auxiliary feedwater system to ensure the required flow to at least two steam generators in the event of a single failure (also see failure analyses, tables 7.3-6 and 10.4-14).

F. Diversity

The auxiliary feedwater system is diversified by utilizing one turbine-driven pump and two motor-driven pumps with air-operated valves. Diversity in automatic actuation signals is provided as seen in figure 7.3-3.

No ac power is required for support of the turbine-driven auxiliary feedwater train.

G. Actuated devices

Table 7.3-19 (items 5 and 6), as well as table 7.3-7, lists the actuated devices.

H. Supporting systems

The Class 1E electric system is required for auxiliary feedwater control. The pressurized air supply required for motive force is normally supplied from the manual instrument air header, which is not safety-related. In the event that the normal air supply is unavailable, the air supply for the auxiliary feedwater motor-driven flow control valves is provided by the safety-related instrument air system.

Each turbine-driven flow control valve is provided with a safety-related air accumulator to supply a limited amount of air to close the flow control valves in the event the normal air supply is unavailable.

I. Portion of system not required for safety

Instrumentation provided for monitoring system performante is not required for safety, with the exception of auxiliary feedwater flow and pump pressure indication that is safety-related.

7.3.3.2.1.2 Design Bases Information.

The design bases of the auxiliary feedwater system, in accordance with Section 3 of IEEE Standard 279 are:

A. Generating station conditions that require protective action:

Auxiliary feedwater is required following a loss of normal feedwater.

B. Range of transient and steady-state conditions of the energy supply and the environment during normal, abnormal, and accident circumstances throughout which the system must perform:

The Class 1E power system is discussed in chapter 8. The auxiliary feed pumps and associated valves are located outside the containment vessel. The control equipment located outside of containment must function through a temperature range of 40 to 120°F, humidity from 10 to 95 percent RH, and atmospheric pressure. The control equipment located inside the control room and auxiliary shutdown panel rooms must function through a temperature range of 68 to 85°F, humidity from 50 to 95 percent RH, and atmosphere pressure.

C. The malfunctions, accidents, or other unusual events that could physically damage protection system components, for which provisions must be incorporated to retain necessary protection system action.

The auxiliary feedwater control system is designed to withstand the effects of a safe shutdown earthquake (SSE) without loss of function. The control system is physically located in such a way to prevent loss of function from missile damage.

D. Minimum performance requirements including system response times, system accuracies, ranges of the magnitudes, and rates of change of sensed variables to be accommodated until proper conclusion of the protection system action.

The system response time will be within 60 seconds from the time of detection of a condition requiring auxiliary feedwater to the time at which the required water flow is achieved.

7.3.3.2.1.3 Final System Drawings

For logic diagrams, see figure 7.3-3. For system piping and instrumentation drawings, see figure 10.4-9.

7.3.3.2.2 Analysis

7.3.3.2.2.1 Conformance to General Design Criteria

A. General Design Criterion 13

Instrumentation and controls necessary to monitor variables and systems over their anticipated ranges for normal plant operating condition are provided in the main control room. Instrumentation and controls necessary to assure adequate safety during accident condition are provided in the main control room and on the emergency shutdown panel. A description of the surveillance instrumentation is provided in section 7.5.

B. General Design Criterion 19

All controls and indications required for safe shutdown of the reactor are provided in the main control room. In the event that the main control room must be evacuated, adequate controls and indications are located outside the main control room to (1) bring to and maintain the reactor in a safe hot shutdown condition.

and (2) provide potential capability to achieve cold shutdown with appropriate procedures.

The emergency shutdown panel, located outside the main control room, is described in paragraph 7.4.1.3.

C. General Design Criterion 34

The auxiliary feedwater system provides an adequate supply of feedwater to the steam generators to remove reactor decay heat following reactor trip. Two steam generators with auxiliary feedwater supply are sufficient to remove reactor decay heat without exceeding design conditions of the RCS.

7.3.3.2.2.2 Conformance to Regulatory Guides

A. Regulatory Guide 1.22

The auxiliary feedwater system and controls are designed to allow periodic testing satisfying technical specification requirements.

B. Regulatory Guide 1.29

The auxiliary feedwater system controls are designed to withstand the effects of an earthquake without loss of function or physical damage. The auxiliary feedwater control system is classified as Seismic Category I in accordance with the guide.

7.3.3.2.2.3 Conformance to IEEE Standard 279

The auxiliary feedwater system controls are designed to conform to the applicable portions of IEEE Standard 279. The control and actuation circuits are designed such that any single failure will not prevent proper protective action (adequate feedwater supply) when required. This is accomplished by redundant systems. Each auxiliary motor-driven feedwater train utilizes control power from independent Class 1E power systems. To prevent interaction between the independent systems, the control channels are separated, with no electrical connections between control channels.

7.3.3.2.2.4 Conformance to Other Criteria, Guides, and Standards

Conformance to other criteria, guides, and standards is indicated on table 7.1-2 and subsection 10.4.9.

7.3.3.2.2.5 Failure Modes and Effects Analysis. Failure modes and effects analysis is given in table 7.3-6.

7.3.3.2.2.6 Periodic Testing. Periodic testing of mechanical equipment associated with this system is discussed in subsection 10.4.9. Provisions for periodic testing of the actuation system are discussed in ITS Chapter 1. 848

7.3.3.3 Containment Spray Actuation

Containment spray which, except for Hi-3 containment pressure I initiation, is in the balance of plant scope, is accomplished through the use of the containment spray system described in subsection 6.2.2 and is shown in figure 6.2-42.

The containment spray system operates subsequent to the design basis accident (DBA). The system is started either manually or by Hi-3 containment pressure (See figure 7.2-1, sheet 8).

The containment spray system has two phases of operation. In the first (injection) phase, the containment spray pumps take suction from the RWST and discharge to the spray headers. In the second (recirculation) phase, the containment spray pumps take suction from the containment ESF sumps and discharge to the spray headers.

During normal operation, the motor-operated valves in the containment spray pump suction lines from the RWST are normally open. The suction valves from the containment ESF sumps and the containment spray pump discharge valves to the spray headers are normally closed. The redundant motor-operated valves from the spray additive tank to the containment spray pump suction lines are normally closed.

On initiation of the containment spray actuation (CSA), the following system functions are performed automatically:

A. Containment spray pump discharge valves are opened to the spray header.

B. Containment spray pumps are started (suction valves from the RWST are normally open).

C. Containment spray additive tank discharge valves are opened.

This system lineup allows the water from the RWST to be pumped to the spray headers, thus completing the first phase of containment spray.

The second phase of containment spray (recirculation phase) is manually initiated on RWST empty level alarm for each fluid train. The following functions are performed:

A. Containment spray suction valves from the containment ESF sump are opened.

B. Containment spray suction valves from the RWST are closed.

This system lineup allows water from the ESF sump to be recirculated to the spray headers, thus completing the second phase of containment depressurization.

The instrumentation provided for monitoring system performance is as follows:

A. Four redundant RWST wide range level indicators with low-low, and empty alarms

B. Containment spray pump discharge pressure indication on each train

C. Containment spray pump discharge flow indication on each train

D. Containment ESF sump level indication on each train with high- and high-high alarms

E. Containment spray additive tank level indication with low- and low-low alarms. The plant computer receives the level signal and provides a separate low- and low-low alarm as well as a non-Class 1E level indication.

Periodic testing and recalibration of items A, D, and E above, along with system testing, will ensure their availability and proper operation. Ranges and accuracies can be found in table 7.5-1.

7.3.3.4 Containment Purge Isolation Actuation System

7.3.3.4.1 Description

The containment area may suffer radioactive contamination in the event a fuel assembly should be severely damaged during handling.

The containment purge isolation system detects any abnormal amount of radioactivity in the containment atmosphere or in the containment purge effluent, and initiates appropriate action to ensure that any release of radioactivity to the

environs is controlled. The containment purge system is also isolated by CIS-A.

7.3.3.4.1.1 System Description

A. Initiating circuits

Four separate, independent radioactivity detectors, one monitoring the refueling bridge machine area atmosphere, one sampling the containment purge exhaust flow and two monitoring the containment atmosphere, provide, upon detection of high radiation levels, signals to bistable units which produce redundant trip signals to the automatic actuation logic. SIS is also provided to the automatic actuation logic. Pretrip alarm and channel failure alarm on downscale signals are provided for all of the monitors.

B. Logic

The containment purge isolation actuation system utilizes one-out-of-two logic to actuate containment purge isolation when required.

C. Bypass

Indication of system bypass is provided as described in section 7.5.

D. Interlocks

There are no interlocks on these controls.

E. Sequencing

There is no automatic sequencing of operation.

F. Redundancy

Controls are provided on a one-to-one basis with the mechanical equipment so that the controls preserve the redundancy of the mechanical equipment.

G. Diversity

Diversity of sensing is provided in that containment purge isolation can be actuated by either the containment refueling bridge machine area monitor by the containment purge exhaust monitor and by the two containment high range area radiation monitors.

H. Actuated devices

Table 7.3-19 (item 2) and table 7.3-8 list the actuated devices.

I. Supporting systems

Supporting systems for the containment purge isolation actuation are the two 120V ac. Class 1E. instrument power supplies discussed in section 8.3. the four 125V dc power supplies discussed in section 8.3. and the instrument air system described in subsection 9.3.1. The isolation function is fail-safe with respect to all of these support systems. that is to say. loss of these support systems will not prevent isolation.

7.3.3.4.1.2 Design Bases Information

The design bases for the containment purge isolation actuation system are described in subparagraph 6.2.4.1.1 (bases 3. 5. and 7).

Additionally. subparagraph 7.3.3.8.1.2 will be considered for the control system components.

7.3.3.4.1.3 Final System Drawings

Diagrammatic descriptions of the containment purge isolation system are given in the following drawings:

A. Figure 7.3-5. logic diagram

B. Figure 9.4-8. piping and instrumentation diagram.

7.3.3.4.2 Analysis

A. Conformance to General Design Criteria

The applicable criteria are indicated in section 7.1. No deviations or exceptions to those criteria are taken.

B. Conformance to other criteria and standards

The design of the control system conforms to the standards listed and discussed in subparagraph 7.3.3.8.2.D.

C. Failure modes and effects analysis

See table 7.3-9 for failure modes and effects analysis.

D. Periodic testing

Periodic testing of the mechanical equipment associated with this system is discussed in subsection 9.4.7. Periodic testing of actuation system is discussed in ITS Chapter 1.

348

7.3.3.5 Fuel Building Emergency Exhaust System

7.3.3.5.1 Description

If a fuel assembly is damaged severely enough to rupture its cladding, fission products can be released and cause the surrounding area's radioactivity level to go considerably above an acceptable level. If this happens in the fuel building, the fuel building exhaust gaseous radiation monitor, or the spent fuel pool area radiation monitor, will detect this abnormal radioactivity level and initiate fuel building emergency ventilation (FBEVS) signal that will place the fuel building ventilation system in an operating mode that meets the following requirement:

A. Isolate normal ventilation.

B. Initiate operation of the emergency exhaust system to maintain the fuel building atmosphere at a negative pressure.

C. Reduce the flow of fuel building air to the outside atmosphere to a minimum consistent with maintaining the required building negative pressure.

D. Filter the exhaust air through HEPA and charcoal filter.

A description of fuel building ventilation system is given in subsection 9.4.6.

7.3.3.5.1.1 System Description

A. Initiating circuits

One radioactivity gas detector on the fuel building ventilation exhaust line and the spent fuel pool area monitor provide diverse radioactivity signals that produce two redundant signals for the automatic

actuation logic. Pretrip alarm and channel failure alarm on downscale signals are also provided for all of the monitors. The emergency exhaust system is on standby for an automatic start following receipt of FBEV signal. 2

The radioactivity signals and the alarm and trip bistable outputs are furnished to the station computer system and the trip status light on the main control panel through isolation circuitry. Alarms and trips are also provided to the station annunciator system through isolation devices.

B. Logic

The control logic for the fuel building emergency ventilation isolation system is shown on figure 7.3-6.

C. Bypass

Indication of system bypass is provided as discussed in section 7.5.

D. Interlocks

There are no interlocks on these controls.

E. Sequencing

There is no automatic sequencing of operation.

F. Redundancy

Controls are provided on a one-to-one basis with the mechanical equipment so that the controls preserve the redundancy of the mechanical equipment.

G. Diversity

Diversity of control is provided in that the fuel building ventilation isolation system can be actuated by either automatic signals or manual control.

H. Actuated devices

Table 7.3-10 and table 7.3-19 (item 1) list the actuated devices.

I. Supporting systems

Supporting systems for the fuel building ventilation isolation system actuation are the four 120V ac instrument power supplies, the four 125V dc power supplies discussed in section 8.3, and the instrument air system which is described in subsection 9.3.1. The isolation function is fail-safe with respect to all of these support systems: that is to say, loss of these support systems will not prevent isolation.

7.3.3.5.1.2 Design Bases Information

The design bases for the fuel building ventilation isolation actuation system are discussed in subparagraph 9.4.2.1.1.

Additionally, subparagraph 7.3.3.8.1.2 is applicable for the control system components.

7.3.3.5.1.3 Final System Drawings

Diagrammatic descriptions of the fuel building ventilation isolation system are given in the following drawings:

A. Figure 7.3-6, logic diagram

B. Figure 9.4-6, piping and instrumentation diagram.

7.3.3.5.2 Analysis

A. Conformance to general design criteria

The applicable criteria are indicated in section 7.1. No deviations or exceptions to those criteria are taken.

B. Conformance to Regulatory Guide 1.25

Conformance with Regulatory Guide 1.25 is discussed in appendix 3A.

C. Conformance to IEEE Standard 279[4]

The design of the control system conforms to the applicable requirements of IEEE Standard 279 as listed in subparagraph 7.3.3.8.2.C.

D. Conformance to other criteria and standards

The design of the control system conforms to the standards listed in paragraph 7.3.3.8.2.D.

E. Failure modes and effects analysis

See table 7.3-11 for failure modes and effects analysis.

F. Periodic testing

Periodic testing of mechanical equipment associated with this system is discussed in subsection 9.4.6. Provisions for the periodic testing of the actuation system are discussed in ITS Chapter 1. |44

7.3.3.6 Control Room Emergency Ventilation

7.3.3.6.1 Description

The normal intake and discharge of air to the control room is transferred to the emergency mode following a LOCA. Air is supplied and recirculated through the control room emergency filtration trains while maintaining the control room at a slightly positive pressure.

7.3.3.6.1.1 System Description

A. Initiating circuits

Two independent and redundant radiation monitors are provided to monitor the control building normal outside air intake. Outputs from each of the two monitors are alarmed in the control room. Sensitivity and response time of these monitors are listed in table 7.3-12. Control room emergency ventilation is initiated by (BOP ESFAS) CREVS.

B. Logic

The control room ventilation system utilizes a one-out-of-two logic as shown in figure 7.3-7.

C. Bypass

Indication of system bypass is provided as described in section 7.5.