# Exhibit FP No. 12

# CHAPTER 7

# INSTRUMENTATION AND CONTROL

## 7.1 GENERAL DESIGN CRITERIA

Complete supervision of both the nuclear and turbine-generator sections of the plant is accomplished by the instrumentation and control systems from the control room. The instrumentation and control systems are designed to permit periodic on-line test to demonstrate the operability of the reactor protection system.

Criteria applying in common to all instrumentation and Control Systems are given in Section 7.1.1. Thereafter, criteria which are specific to one of the instrumentation and control systems are discussed in the appropriate portion of the description of that system, as referenced in Section 7.1.2.

The General Design Criteria presented and discussed in this section are those which were in effect at the time when Indian Point 3 was designed and constructed. These general design criteria, which formed the bases for the Indian Point 3 design, were published by the Atomic Energy Commission in the Federal Register of July 11, 1967, and subsequently made a part of 10 CFR 50.

The Authority has completed a study of compliance with 10 CFR Parts 20 and 50 in accordance with some of the provisions of the Commission's Confirmatory Order of February 11, 1980. The detailed results of the evaluation of compliance of Indian Point 3 with the General Design Criteria presently established by the Nuclear Regulatory Commission (NRC) in 10 CFR 50 Appendix A, were submitted to NRC on August 11, 1980, and approved by the Commission on January 19, 1982. These results are presented in Section 1.3.

### 7.1.1 Instrumentation and Control Systems Criteria

Instrumentation and Control Systems

Criterion: Instrumentation and controls shall be provided as required to monitor and maintain within prescribed operating ranges essential reactor facility operating variables. (GDC 12 of 7/11/67)

Instrumentation and controls essential to avoid undue risk to the health and safety of the public are provided to monitor and maintain neutron flux, primary coolant pressure, flow rate, temperature, and control rod positions within prescribed operating ranges.

The non-nuclear regulating process and containment instrumentation measures temperatures, pressure, flow, and levels in the Reactor Coolant System, Steam Systems, Containment and other Auxiliary Systems.

Process variables required on a continuous basis for the startup, power operation, and shutdown of the plant are controlled form and indicated or recorded at the control room, access to which is supervised. The quantity and types of process instrumentation provided ensure safe and orderly operation of all systems and processes over the full operating range of the plant.

### 7.1.2 Related Criteria

The following are criteria which are related to all instrumentation and control systems but are more specific to other plant features or systems, and therefore are discussed in other chapters, as listed.

| Title of Criterion (7/11/67 issue) | Reference |
|---|---|
| Suppression of Power Oscillations (GDC 7) | Chapter 3 |
| Reactor Core Design (GDC 6) | Chapter 3 |
| Quality Standards (GDC 1) | Chapter 4 |
| Performance Standards (GDC 2) | Chapter 4 |
| Fire Protection (GDC 3) | Chapter 5 and 9 |
| Missile Protection (GDC 40) | Chapters 4, 5, and 6 |
| Emergency Power (GDC 39 and GDC 24) | Chapter 8 |

## 7.2 PROTECTIVE SYSTEMS

The protective systems consist of both the Reactor Protection System and the Engineered Safety Features. Equipment supplying signals to any of these protective systems is considered a part of that protective system.

### 7.2.1 Design Bases

The General Design Criteria presented and discussed in this section are those which were in effect at the time when Indian Point 3 was designed and constructed. These general design criteria, which formed the bases for the Indian Point 3 design, were published by the Atomic Energy Commission in the Federal Register of July 11, 1967, and subsequently, made a part of 10 CFR 50.

The Authority has completed a study of compliance with 10 CFR Parts 20 and 50 in accordance with some of the provisions of the Commission's Confirmatory Order of February 11, 1980. The detailed results of the evaluation of compliance of Indian Point 3 with the General Design Criteria presently established by the Nuclear Regulatory Commission (NCR) in 10 CFR 50 Appendix A, were submitted to NRC on August 11, 1980 and approved by the Commission on January 19, 1982. These results are presented in Section 1.3.

Control Room

Criterion: The facility shall be provided with a control room from which actions to maintain safe operational status of the plant can be controlled. Adequate radiation protection shall be provided to permit continuous occupancy of the control room under any credible post-accident condition or as an alternative, access to other areas of the facility as necessary to shut down and maintain safe control of the facility without excessive radiation exposure of personnel. (GDC 11 of 7/11/67)

Indian Point 3 is equipped with a Control Room which contains those controls and instrumentation necessary for operation of the reactor and turbine generator under normal and accident conditions.

The Control Room is provided with emergency lighting; color coding, labeling and demarcation of reactor coolant control and display panels; switch protection; and other aids as required to ensure proper operation of the reactor, turbine generator and auxiliaries under all operating and accident conditions.

The Control Room is continuously occupied by qualified operating personnel under all operating and Maximum Credible Accident (MCA) conditions. The Post Accident Monitoring instrumentation available to the operator for monitoring plant conditions is provided in Table 7.5-1. The instrumentation complies with Regulatory Guide 1.97 requirements, as documented in NRC Letter, J.D. Neighbors to R. Beedle, dated 4/3/91, entitled "Emergency Response Capability – Conformance To RG 1.97 Revision 3, for Indian Point 3" (TAC No. 51099).

The instrumentation originally available to the operator for monitoring conditions in the Reactor, Reactor Coolant System and the Containment Building are provided in Historical Tables 7.2-4 and 7.2-5.

Historical Table 7.2-4 lists indication (meters, recorders, etc.) available for providing information following moderate and infrequent faults as originally analyzed in Chapter 14. Similarly, Historical Table 7.2-5 relates to limiting faults such as a LOCA as originally analyzed in Chapter 14.

The design criteria used in the selection of the original readouts were:

1) The range of readouts extend over the maximum expected range of the variable being measured as a result of faults originally analyzed in Chapter 14.

2) The combined indicated accuracies are within the errors originally assumed in the safety analysis.

Sufficient shielding, distance, and containment integrity are provided to assure that control room personnel shall not be subjected to doses under postulated accident conditions during occupancy of, ingress to and egress from the Control Room which, in the aggregate, would exceed that limits in 10 CFR 100. The control room ventilation consists of a system having a large percentage of recirculated air. The fresh air intake can be closed automatically or by manual backup to stop the intake of airborne activity if monitors indicate that such action is appropriate.

Core Protection Systems

Criterion: Core protection systems, together with associated equipment, shall be designed to prevent or to suppress conditions that could result in exceeding acceptable fuel damage limits. (GDC 14 of 7/11/67)

The basic reactor tripping philosophy is to define a region of power and coolant temperature conditions allowed by the primary tripping functions, the overpower ΔT trip, the overtemperature ΔT trip and the nuclear overpower trip. The allowable operating region within these trip settings

is provided to prevent any combination of power, temperatures and pressure which would result in DNB with all reactor coolant pumps in operation. Additional tripping functions such as a high pressurizer pressure trip, low pressurizer pressure trip, high pressurizer water level trip, loss of flow trip, steam and feed-water flow mismatch trip, steam generator low-low water level trip, turbine trip, safety injection trip, nuclear source and intermediate range trips, and manual trip are provided as backup tot he primary tripping functions for specific accident conditions and mechanical failures.

A dropped rod signal blocks automatic rod withdrawal and also provides a turbine load cutback if above a given power level. The dropped rod is indicated from individual rod position indicators or by a rapid flux decrease on any of the power range nuclear channels.

Over power $\Delta T$, overtemperature $\Delta T$, and $T_{avg}$ deviation rod stops prevent abnormal power conditions which could result from excessive control rod withdrawal initiated by a malfunction of the Reactor Control System or by operator violation of administrative procedures.

Engineered Safety Features Protection Systems

Criterion: Protection systems shall be provided for sensing accident situations and initiating the operation of necessary engineered safety features (GDC 15 of 7/11/67).

Instrumentation and controls provided for the protective systems are designed to trip the reactor in order to prevent or limit fission product release from the core, and to limit energy release, to signal containment isolation, and to control the operation of engineered safety features equipment.

The Engineered Safety Features are actuated by the engineered safety features actuation channels. Each coincidence network energizes an engineered safety features actuation device, which operates the associated engineered safety features equipment, motor starters and valve operators. The channels are designed to combine redundant sensors, independent channel circuitry, coincident trip logic and different parameter measurements so that a safe and reliable system is provided in which a single failure will not defeat the protective function. The action initiating sensors, bistables and logic is shown in the figures which are included in the detailed engineered safety features instrumentation description given in the design section for each system. The engineered safety features instrumentation system actuates (depending on the severity of the condition) the Safety Injection System, the Containment Isolation System, the Containment Air Recirculation System, and the Containment Spray System.

The passive accumulators of the Safety Injection System do not require signal or power sources to perform their function. The actuation of the active portion of the Safety Injection System is described later in this section.

The containment air recirculation coolers are normally in use during plant operation. These units are, however, in the automatic sequence, which actuates the engineered safety features upon receiving the necessary actuating signals indicating an accident condition. The fan cooler bypass valves open on a safety injection signal to provide maximum service water flow.

Containment spray is actuated by coincident and redundant high containment pressure signals (high-high level).

The Containment Isolation System provides the means of isolating the various pipes passing through the containment walls as required to prevent the release of radioactivity to the outside environment in the event of a Loss-of-Coolant Accident.

Protection Systems Reliability

Criterion: Protection systems shall be designed for high functional reliability and in-service testability necessary to avoid undue risk to the health and safety of the public. (GDC 10 of 7/11/67)

The reactor uses the high speed version of the Westinghouse magnetic-type control rod drive mechanisms. Upon a loss of power to the coils, the Rod Cluster Control (RCC) assemblies with full length absorber rods are released and fall by gravity into the core.

The reactor internals, fuel assemblies and drive system components were designed as seismic Class I equipment. The RCC assemblies are fully guided through the fuel assembly and for the maximum travel of the control rod into the guide tube. Furthermore, the RCC assemblies are never fully withdrawn from their guide thimbles in the fuel assembly. For this reason, and because of the flexibility designed into the RCC assemblies, abnormal loadings and misalignments can be sustained without impairing operation of the RCC assemblies.

The Rod Cluster Control assembly guide system is locked together with pins throughout its length to ensure against misalignments which might impair control rod movement under normal operating conditions and credible accident conditions. An analogous system has successfully undergone 4132 hours of testing in the Westinghouse Reactor Evaluation Center during which about 27,200 feet of step-driven travel and 1461 trips were accomplished with test misalignments in excess of the maximum possible misalignment experienced when installed in the plant.

All primary reactor trip protection channels required during power operation are supplied with sufficient redundancy to provide the capability for channel calibration and test at power.

Removal of one trip circuit is accomplished by placing that circuit in a tripped mode i.e., a two-out-of-three circuit becomes a one-out-of-two circuit. A Channel bistable may also be placed in a bypassed mode, i.e., a two-out-of-three circuit becomes a two-out-of-two circuit. Testing in a bypassed mode does not trip the system even if a trip condition exists in a concurrent channel.

Reliability and independence are obtained by redundancy within each tripping function. In a two-out-of-three circuit, for example, the three channels are equipped with separate primary sensors. Each channel is continuously fed from its own independent electrical source. Failure to de-energize a channel when required would be a mode of malfunction that would affect only that channel. The trip signal furnished by the two remaining channels would be unimpaired in this event.

Protection Systems Redundancy and Independence

Criterion: Redundancy and independence designed into protection systems shall be sufficient to assure that no single failure on removal from service of any component or channel of such a system will result in loss of the protection function. The redundancy provided shall include, as a minimum, two channels of protection function to be served. (GDC 20 of 7/11/67)

The Reactor Protection Systems were designed so that the most probable modes of failure (loss of voltage, relay failure) in each protection channel result in a signal calling for the protective trip. Each protection system design combines redundant sensors and channel independence with coincident trip philosophy so that a safe and reliable system is provided in which a single failure will not defeat the channel function, cause a spurious plant trip, or violate reactor protection criteria.

The design basis for the Reactor Protection System and Engineered Safety Features equipment radiation exposure was that the equipment must function after the exposure associated with the TID-14844 model accident. The maximum anticipated exposure for components located within the Containment was calculated to be $1.6 \times 10^8$ rads, which is accumulated during one year following the accident. (Note that the integrated exposure for safeguards equipment during 40 years of operation was calculated to be less than $5 \times 10^5$ rads.) In the determination of exposure, no credit was taken for containment cleanup or other removal mechanism other than isotope decay. The expected integrated exposure on the outside of the Containment Building, again assuming TID-14844 releases and no credit for cleanup, will be less than $10^2$ rads integrated over a year at the containment outside surface.

Protection system instrument cables are divided into four channels. Channeling separation is continuous from instrument sensor to receiver. Bistable or digital type outputs 120 volts AC or 125 volts DC to protection system logic relays are divided into the same four channels.

Power and control cables for engineered safeguards are divided into three basic channel systems. Power and control cabling for reactor trip and containment isolation valves are divided into two channels.

In addition to channels of separation, cables were assigned to individual routing systems in accordance with their voltage level, size, and function. Six independent conduit and tray systems are employed on Indian Point 3 as follows:

1) 6900 volt power

2) Heavy 125 volts DC power cables and heavy 480 volts AC (over 100 hp) power cables

3) Lighting panel feeders and medium power (greater than No 12 AWG wire size) 480 volts AC cables

4) Control and light (non-heavy) power cables

5) Instrument cables

6) Rod control cables

Conduit fill for all systems is based on standard national Electric Code Recommendations. Criteria for tray fill are given in Section 8.2

Cables in the conduit and cable schedule are identified by a circuit code, in addition to their routing, to assure that the cable will be installed in the proper tray systems, as well as the proper channel.

Separation of channels was established throughout the plant by the use of separate trays or conduits (exceptions are documented and justified in Reference 1). In addition, whenever a heavy power tray was located less than three feet beneath any tray of a different channel, a transit fire barrier was installed between the trays. A vertical barrier was installed where trays of different channels were installed less than one foot apart, horizontally. Vertically barriers and fire wraps were installed to separate cables and equipment and associated non-safety circuits of redundant trains to protect against radiant energy from a 10 CFR 50, Appendix R assumed fire. Additionally, a horizontal barrier was installed where trays (other than heavy power) were installed less than one foot beneath any tray of a different channel.

In the area of the electrical tunnel between the Control Building and Containment Building and containment penetration area, two tunnels provide the separation for the four channels. A cross section of this portion of the tunnel is shown in the Plant Drawing 9321-F-31193 [Formerly Figure 7.2-18].

In general, control board switches with their associated indicating lights are contained in a modularized structure which provides physical separation between power "trains." Where more than one train is required to connect to a single switch, the wiring is routed to different quadrants within the module itself. Separate connectors for each redundant circuit are used, and board wiring is channelized to separate terminal blocks contained in individual channelized vertical risers located above separated floor slots. The wiring "trains" within the board are divided into three separate groups. Train "X" is that wiring which is associated with buses fed from diesel generator No. 32, Train "Y" is that wiring which is associated with buses fed from diesel generator No. 33 and Train "Z" is that wiring which is associated with buses fed from diesel generator No. 31. These "trains" are physically separated from each other by horizontal raceways which route the wiring to its appropriate vertical riser.

The wiring of local control panels which contain cabling from different channels have been separated by interior metal barriers or were separated into more than one panel. The main three phase power circuits are protected by means of three-pole breakers. Individual small power feeds from the motor control centers have three phase protection by means of fuses and "heater" overload devices. Single phase circuits are protected by single pole devices including fuses and/or breakers. (See Section 8.2)

Channel independence is carried throughout the system extending from the sensor to the relay actuating the protective function. The protective and control functions are fully isolated, control being derived from the primary protection signal path through an isolation amplifier. As such, a failure in the control circuitry does not affect the protection channel. This approach is used for pressurizer pressure and water level channels, steam generator water level, $T_{avg}$ and $\Delta T$ channels, steam flow-feedwater flow and nuclear instrumentation channels.

The analog type equipment associated with the Reactor Protection and Engineered Safety Features Systems is considered to be the most susceptible to temperature effects because of the accuracies involved. Excessive temperature for long periods in areas containing switchgear, cables, etc. would result in a slight degradation of life but would not affect performance. The Control Room is the limiting case for reactor shutdown with regard to electrical equipment. The protective equipment in the control and relay rooms was designed to operate in an environment up to 120°F without loss of function.

Temperature in the Control Room and adjoining equipment room is maintained for personnel comfort at 70 ± 10°F. Protective equipment in this space was designed to operate within a design tolerance over this temperature range. Design specifications for this equipment specified no loss of protective function up to 120°F. Exceptions to this are evaluated in NSE 95-3-032, Revision 1 (See FSAR Section 9.9.2). Thus, there is a wide margin between design limits and the normal operating environment for control room equipment.

The engineered safety features equipment is actuated by one or the other of the engineered safety features actuation channels. Each coincidence network actuates an engineered safety actuation device that operates the associated engineered safety features equipment, motor starters and valve operators. As an example, the control circuit of a safety injection pump is typical of the control circuit for a large pump operated from switchgear. The actuation relay, energized by the Engineered Safety Features Instrumentation System, has normally open contracts. These contacts energize the circuit breaker closing coil to start the pump when the control relay is energized. The Engineered Safety Features Instrumentation System actuates (depending on the severity of the condition) the Safety Injection System, the Containment Isolation System, Containment Air Recirculation System and Containment Spray System.

In the Reactor Protection System, two reactor trip breakers are provided to interrupt power to the full length rod drive mechanisms. The breaker main contacts are connected in series (with power supply) so that opening either reactor trip breaker interrupts power to all full length rod mechanisms, permitting them to fall by gravity into the core.

In the event of a loss of reactor trip breaker control power, the reactor trip breaker under voltage coils and associated relays are de-energized and the breakers trip to an open mode. An electrical interlock prevents both bypass breakers from being closed concurrently.

Further detail on redundancy is provided through the detailed descriptions of the respective systems covered by the various sections in this chapter. In summary, reactor protection was designed to meet all presently defined reactor protection criteria and is in accordance with the IEEE-279-1971, "Standard for Nuclear Plant Protection Systems."

Required continuous electrical supply is discussed in Chapter 8.

Demonstration of Functional Operability of Protection Systems

Criterion: Means shall be included for suitable testing of the active components of protection systems while the reactor is in operation to determine if failure or loss of redundancy has occurred. (GDC 25 of 7/11/67)

The analog equipment of each protection channel in service at power is capable of being tested and tripped independently by simulated analog input signals to verify its operation. The trip logic circuitry includes means to test each logic channel through to the trip breakers. Thus, the operability of each trip channel can be determined conveniently and without ambiguity.

Testing of the diesel-generator starting may be performed from the diesel generator control board. The generator breaker is not closed automatically after starting during this testing. The generator may be manually synchronized to the 480 Volt bus for loading. Complete testing of the starting of diesel generators can be accomplished by tripping the associated 480 Volt undervoltage relays and providing a coincident simulated safeguards signal. The ability of the

units to start within the prescribed time and to carry load can be periodically checked. (The Electrical Systems are discussed in more detail in Section 8.2.3.)

The reactor coolant pump breakers open trip is not testable at power; it is a backup trip which is testable only during shutdown. Testing at power (opening the breakers) would involve a loss of flow in the associated loop.

Protection Against Multiple Disability for Protection Systems

Criterion: The effects of adverse conditions to which redundant channels or protection systems might be exposed in common, either under normal conditions or those of an accident, shall not result in loss of the protection function or shall be tolerable on some basis. (GDC 23 of 7/11/67)

The components of the protection system were designed and laid out so that the mechanical and thermal environment accompanying any emergency situation in which the components are required to function does not interfere with that function.

Separation of redundant analog protection channels originates at the process sensors and continues back through the field wiring and containment penetrations to the analog protection racks. Physical separation is used to the maximum practical extent to achieve separation of redundant transmitters. Separation of field 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 redundant components in different protection racks. Each redundant channel is energized from a different vital instrument bus.

Protection System Failure Analysis Design

Criterion: The protection systems shall be designed to fail into a safe state or into a state established as tolerable on a defined basis if conditions such as disconnection of the system, loss of energy (e.g., electrical power, instrument air), or adverse environments (e.g., extreme heat or cold, fire, steam, or water) are experienced. (GDC 26 of 7/11/67)

Each reactor trip circuit was designed so that trip occurs when the circuit is de-energized; therefore, loss of channel power causes the system to go into its trip mode. In a two-out-of-three circuit, the three channels are equipped with separate primary sensors and each channel is energized from an independent electrical bus. Failure to de-energize when required is a mode of malfunction that affects only one channel. The trip signal furnished by the two remaining channels is unimpaired in this event.

Reactor trip is implemented by interrupting power to the magnetic latch mechanisms on all drives allowing the full length rod clusters to insert by gravity. The protection system is thus inherently safe in the event of a loss of power.

The engineered safety features actuation circuits were designed on the "energize to operate" principle unlike the reactor trip circuits.

The steam line isolation signal on high-high containment pressure, which uses the same circuitry as the containment spray actuation signal, was also designed on the "energize to operate" principle. There are a total of six high-high containment pressure instruments which

are separated into three channels. The three high-high containment pressure instrument channels are powered from three separate independent sources (one channel from instrument Bus No. 31 powered from Battery No. 31, the second channel from instrument Bus No. 33 powered from Battery No. 33, and the third channel from instrument Bus No. 34 powered from Instrument Bus No. 34 powered from Battery No. 34 with alternate supply from safeguards Motor Control Center No. 36B).

This assures operation of a sufficient number of containment pressure instruments in the event of a power failure to one of the instrument channels.

In the event that power to any instrument bus is lost, there is no single failure that could occur to prevent any protective action. Reactor trip initiation signals are de-energized to actuate. The containment spray initiation signals, of which only two of three are required, are powered from three separate power sources (i.e., Instrument Buses No. 31, No. 33, and No. 34).

If power would ever be lost to any instrument bus, channel trip annunciators, etc. associated with the protective functions powered from this bus would alarm. This would mean to the operator that this one complete protective channel is in the trip mode. The event would be indicative of the loss of power for this particular channel of protective devices.

The above design is consistent with all of the instrument buses regardless of their source of power, as the loss of any one instrument bus, for any reason, would give channel trip alarms and indications for the respective channel of protection devices. These alarms would be a true indication because on loss of instrument power the associated protective channel is indeed in the trip mode. This complies with the requirements of Section 4.20 of IEEE-279. (See Section 8.2)

Each emergency diesel-generator is started by undervoltage on its associated 480 Volt bus or by the safety injection signal independent of the other 480 Volt buses and diesel generators. Engine cranking is accomplished by a stored energy system supplied solely for the associated diesel generators. The undervoltage relay scheme was designed so that loss of 480 Volt power does not prevent the relay scheme from functioning properly.

Redundancy of Reactivity Control

Criterion: Two independent control systems, preferably of different principles, shall be n provided. (GDC 27 of 7/11/67)

One of the two Reactivity Control Systems employs rod cluster control assemblies to regulate the position of Ag-In-Cd neutron absorbers within the reactor core. The other Reactivity Control System employs the Chemical and Volume Control System to regulate the concentration of boric acid solution (neutron absorber) in the Reactor Coolant System.

A detailed description of the Reactivity Control System for Indian Point 3, sufficient to demonstrate redundancy and capability as established under the provisions of this criterion, is presented in Section 3.1.

Reactivity Control Systems Malfunction

Criterion: The reactor protection system shall be capable of protecting against any single malfunction of the reactivity control system, such as unplanned continuous

withdrawal (not ejection or dropout) of a control rod, by limiting reactivity transients to avoid exceeding acceptable fuel damage limits. (GDC 31 of 7/11/67)

Reactor shutdown with rods is completely independent of the normal control functions since the trip breakers completely interrupt the power to the full length rod mechanisms regardless of existing control signals. Effects of continuous withdrawal of a rod control assembly and of deboration are described in Sections 7.3.1, 7.3.2, 9.2 and 14.1.

Principles of Design

Redundancy and Independence

The protective systems are redundant and independent for all vital inputs and functions. Each channel is functionally independent of other redundant channels and is supplied from an independent power source. Isolation of redundant protection channels is described in further detail elsewhere in this section and in Section 7.2.2.

Manual Actuation

Means are provided for manual initiation of protective system action. Failures in the automatic system do not prevent the manual actuation of protective functions. Manual actuation requires the operation of a minimum of equipment.

Channel Bypass or Removal from Operation

The system was designed to permit any one channel to be maintained and when required, tested or calibrated during power operation without system trip. During such operation the active parts of the system continue to meet the single failure criterion. Since the channel under test is either tripped or superimposed, test signals are used which do not negate the process signal.

It should be noted that the "one-out-of-two" logic systems are permitted to violate the single failure criterion during channel bypass, provided that acceptable reliability of operation can be otherwise demonstrated and bypass time interval is short.

Capability for Test and Calibration

The bistable portions of the protective system (e.g., relays, bistables, etc.) provide trip signals only after signals from analog portions of the system reach preset values.

Capability is provided for calibrating and testing the performance of the bistable portion of protective channels and various combinations of the logic networks during reactor operation.

The analog portion of a protective channel provides analog signals proportional to a reactor or plant parameter. The following means are provided to permit checking the analog portion of a protective channel during reactor operation:

a) Varying the monitored variable

b) Introducing and varying a substitute transmitter signal

c) Cross checking between identical channels or between channels which bear a known relationship to each other and which have readouts available.

The design permits the administrative control of the means for manually by-passing channels or protective functions.

The design permits the administrative control of access to all trip settings, module calibration adjustments, test points, and signal injection points.

Information Readout and Indication of Bypass

The protective systems were designed to provide the operator with accurate, complete, and timely information pertinent to their own status and to plant safety.

Indication is provided in the Control Room if some part of the system has been administratively bypassed or taken out of service.

Trips are indicated and identified down to the channel level.

Vital Protective Functions and Functional Requirements

The Reactor Protective System monitors parameters related to safe operation and trips the reactor to protect the reactor core against fuel rod cladding damage caused by departure from nucleate boiling (DNB) and to protect against Reactor Coolant System damage caused by high system pressure. The engineered safety features instrumentation system monitors parameters to detect failure of the Reactor Coolant System and initiates containment isolation and engineered safety features operation to contain radioactive fission products.

This section covers those protective systems provided to:

a) Trip the reactor to prevent or limit fission product release from the core and to limit energy release.

b) Isolate containment and activate the Isolation Valve Seal Water System when necessary.

c) Control the operation of engineered safety features provided to mitigate the effects of accidents.

The core protective systems in conjunction with inherent plant characteristics were designed to prevent anticipated abnormal conditions from causing fuel damage exceeding limits established in Chapter 3 or Reactor Coolant System damage exceeding effects established in Chapter 4.

Completion of Protective Action

Where 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 part of the protective system and were designed in accordance with the criteria of this section.

The protective systems were designed so that once initiated, a protective action goes to completion. Return to normal operation requires administrative action by the operator.

Multiple Trip Settings

Where it is necessary to change to a more restrictive trip setting to provide adequate protection for a particular mode of operation or set of operating conditions, the design provides positive means of assuring that the more restrictive trip setting is used. The devices used to prevent improper use of less restrictive trip settings are considered a part of the protective system and were designed in accordance with the other provisions of these criteria.

Interlocks and Administrative Procedures

Interlocks and administrative procedures required to limit the consequences of fault conditions other than those specified as limits for the protective function comply with the protective function comply with the protective system criteria.

Protective Actions

The Reactor Protective System automatically trips the reactor to protect the reactor core under the following conditions:

a) The reactor power, as measured by neutron flux, reaches a pre-set limit.

b) The temperature rise across the core, as determined from loop $\Delta T$, reaches a limit either from an overpower $\Delta T$ set point or an overtemperature $\Delta T$ set point (function of $T_{avg}$ and pressurizer pressure, adjusted by neutron flux distribution). Overtemperature $\Delta T$ set point is adjusted by neutron flux distribution.

c) The pressurizer pressure reaches an established minimum limit.

d) Loss of reactor coolant flow as sensed by low flow, loss of pump power or pump breakers opening.

e) Pressurizer pressure or level trips the reactor to protect the primary coolant boundary when the pressurizer pressure or level reaches an established maximum limit.

Interlocking functions derived from the Reactor Protective System inhibit control rod withdrawal on the occurrence of a specified parameter reaching a value lower than the value at which reactor trip is initiated.

For anticipated abnormal conditions, protective systems in conjunction with inherent plant characteristics and engineered safety features are designed to ensure that limits for energy release to the Containment and for radiation exposure (as in 10 CFR 100) are not exceeded.

Seismic Design Criteria

For either the operational or design basis earthquake, the equipment was designed to assure that it does not lose its capability to perform its function, i.e., shut the plant down and maintain it

in a safe shutdown condition. For the design basis earthquake, permanent deformation of the equipment is acceptable provided that the capability to perform its function is maintained.

7.2.2 System Design

Reactor Protective System Description

Figure 7.2-2 is a block diagram of the Reactor Protective System; Figure 7.2-3 illustrates the core thermal limits and shows the trip points that are used for the protection system. The solid lines are a locus of limiting design conditions representing the core thermal limits at five pressures. The core thermal limits are based on the conditions which yield the applicable limit value for departure from nucleate boiling ratio (DNBR) or those conditions which preclude bulk boiling at the vessel exit. The dashed lines indicate the maximum permissible trip points for the overtemperature high $\Delta T$ reactor trip including allowances for measurement and instrumentation errors.

The maximum and minimum pressures shown (2470 psia and 1750 psia) represent the set points for the high pressure and low pressure reactor trips.

Adequate margins exist between the worst steady state operating point (including all temperature, calorimetric, and pressure errors) and required trip points to preclude a spurious plant trip during design transients.

Indication

All transmitted signals (flow, pressure, temperature, etc.) which can cause a reactor trip are either indicated or recorded for every channel.

Engineered Safety Features Instrumentation Description

Plant Drawings IP3V-0171-0070, IP3V-0171-0056, 5651D72 Sheets 10, 12, and 12A [Formerly Figures 7.2-4, 7.2-5 and 7.2-6] show the action initiating sensors, bistables and logic for the engineered safety features instrumentation.

The engineered safety features actuation system automatically performs the following vital functions:

1) Start operation of the Safety Injection System upon low pressurizer pressure signal or high containment pressure signals (approximately 10% of containment design pressure), or on coincidence of high differential pressure between any two steam generators, 2 sets of 2/3 high-high pressure [energize to actuate], or after time delay (maximum 6 seconds) in coincidence with high steam flow in 2/4 lines in coincidence with (a) low $T_{avg}$ in 2/4 lines or (b) low steam line pressure in 2/4 lines.

2) Operate the containment isolation valves in non-essential process lines upon detection of high containment pressure signals (Phase A containment isolation). The Isolation Valve Seal Water System is actuated upon automatic actuation of the Safety Injection System.

3) Start the Containment Spray System and operate the remaining containment isolation valves upon detection of a containment pressure signal higher than required in item (2) above (Phase B containment isolation; approximately 24 psig).

4) Start operation of the safeguards equipment actuation sequence signal. This includes actuating signals to such components as the Safety Injection System and the Containment Air Recirculation, Cooling and Filtration System.

Steam Line Isolation

Any of the following signals will close all steam line isolation valves:

1) After time delay (maximum 6 seconds) in coincidence with high steam flow in 2/4 lines in coincidence with (a) low $T_{avg}$ in 2/4 lines or (b) low steam line pressure in 2/4 lines.

2) High containment pressure signals (two sets of 2/3 high-high pressure) [energize to actuate].

3) Steam line isolation valves can also be closed one at a time by manual action.

Feedwater Line Isolation

Any safety injection signal will isolate the main feedwater lines by closing all control valves (including associated MOVs) and the pump discharge valves. The closure of the pump discharge valves will cause the main feedwater pumps to trip.

ATWS Mitigating System Actuation Circuitry (AMSAC) Description

The ATWS Mitigating System Actuation Circuitry (AMSAC) is installed at IP3 in accordance with the requirements of 10 CFR 50.62 "Reduction of Risk From Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants." An ATWS is an anticipated operational occurrence (such as loss of feedwater, loss of condenser vacuum, or loss of offsite power) that is accompanied by a failure of the Reactor Protection System (RPS) to shut down the reactor. The ATWS Rule requires specific improvements in the design and operation of commercial nuclear power facilities to reduce the probability of failure to shut down the reactor following anticipated transients and to mitigate the consequences of an ATWS event.

AMSAC provides an alternate means of tripping the turbine and actuating auxiliary feedwater (AFW) flow apart from the reactor protection system (RPS). The AMSAC equipment is reasonably diverse from the existing RPS equipment to minimize the potential for common cause failures. Also, AMSAC logic power supplies and logic circuitry are independent from the RPS power supplies and logic circuitry. The turbine trip and AFW flow actuation will provide adequate assurance that the reactor coolant system (RCS) would not be subject to potential damage as a result of overpressure. The pressure limit (3200 psig) corresponds to the ASME boiler and Pressure Vessel Code Level C Service Limit stress criteria. Past ATWS analyses, see WCAP-8330 for example, show there are only two ATWS transients for which the ASME Service level limit may be approached. These transients are the Complete Loss of Normal Feedwater Without Scram and the Loss of Load Without Scram.

The Complete Loss of Normal Feedwater transient can occur due to the simultaneous tripping of the main feedwater or condensate pumps or the simultaneous closing of the main feedwater control valves or main feedwater pump discharge valves.

The Loss of Load transient considered for ATWS is one in which the vacuum in the main condenser is lost, resulting in a complete loss of normal feedwater. This could occur, for example, if the circulating water pumps trip. The main turbine will then trip on high backpressure as will any turbine-driven main feedwater pump that exhausts into the main condenser.

Since, in both of the above described transients (and in only these transients) the main feedwater is completely lost, the AMSAC is designed to actuate the auxiliary feedwater flow when the complete loss of main feedwater flow is anticipated.

Short-term protection against high reactor coolant system pressures is not required until 70% of nominal power. However, in order to minimize the amount of reactor coolant system voiding during an ATWS, AMSAC operates at and above 40% of turbine power. Furthermore, the potential exists for spurious AMSAC actuations during start-up at the lower power levels. To assure the above requirements are met, AMSAC is automatically blocked at turbine loads less than 40% by the C-20 permissive. In the event of a turbine trip, both turbine power transmitter indications will drop below 40% of full scale turbine power level. A timer in the AMSAC circuitry will maintain the trip permissive (C-20) for 330 seconds to ensure that the AMSAC system is still armed. However, in the event of an ATWS below 40% of nominal load, operator action will be required to provide long-term core protection by initiating auxiliary feedwater flow.

Actuation of AMSAC will occur on low main feedwater flow as measured by the low feedwater flow transmitters. The setpoint to actuate AMSAC is approximately 21% of nominal main feedwater flow. Although 21% flow is more than ample to protect against overpressure in the event of an ATWS, instrumentation error would become unacceptably large if a substantially lower set point were used.

An AMSAC output is initiated after a predetermined time delay whenever turbine power is 40% or greater coincident with three of the four feedwater flow transmitters indicating feedwater flow of 21% or less. The time delay is determined by the highest Turbine Power Level sensed at the time the ¾ low feedwater flow is sensed. 60 second lag units maintain Turbine Power Level close to the pre-turbine trip condition, for determination of the variable time delay. The time delay varies from a maximum of 300 seconds at 40% power to 25 seconds at 100% power (in accordance with the WOG curves). The purpose of this time delay is twofold. First, this time delay allows the reactor protection system to respond initially to a low feedwater flow condition. Secondly, during this time delay, the operator is provided with an AMSAC alert annunciator in the CR. If during the AMSAC alert period the operator increases feedwater flow above 21%, AMSAC will not actuate and the timer will reset. However, once an AMSAC signal is initiated, the signal will be maintained for at least 40 seconds to ensure all required actions occur. Turbine trip, turbine power auxiliary feedwater valve actuation and steam generator isolation and sample valve closure functions are immediately actuated by AMSAC. The motor driven auxiliary feedwater pumps have a 28 second time delay built into their starting circuits. As such, the motor driven auxiliary feedwater pumps will start 28 seconds after an AMSAC signal is initiated. This time delay is in accordance with 10 CFR 50.62 (the AMSAC Rule) which requires that the AMSAC AFW initiation function is performed within 90 seconds following initiation of an AMSAC signal. The AMSAC output signal is energized to actuate, so that a loss of power to the AMSAC cabinet will not initiate an AMSAC trip.

The AMSAC Logic Diagram is shown in Plant Drawing 9321-LL-38077 [Formerly Figure 7.2-19].

Reactor Protective System Safety Features

Separation of Redundant Protection Channels

The Reactor Protection System was designed on a channelized basis to achieve separation between redundant protection channels. The channelized design, as applied to the analog as well as the logic portions of the protection system, is illustrated by Figure 7.2-1 and is discussed below. Although shown for four channel redundancy, the design is applicable to two and three channel redundancy.

Separation of redundant analog channels originates at the process sensors and continues through the field wiring and containment penetrations to the analog protection racks.

Physical separation was used to the maximum practical extent to achieve separation of redundant transmitters. Separation of field wiring was achieved using separate wireways, cable trays, conduit runs and containment penetrations for each redundant channel. Analog equipment was separated by locating redundant components in different protection racks. Each redundant protection set is energized from a separate AC power feed.

The reactor trip bistables are mounted in the protection racks and are the final operational component in an analog protection channel. Each bistable drives two logic relays ("C" & "D"). The contacts from the "C" relays are interconnected to form the required actuation logic for Trip Breaker No. 1 through DC power feed No. 1. The transition from channel identity to logic identity is made at the logic relay coil/relay contact interface. As such, there is both electrical and physical separation between the analog and the logic portions of the protection system. The above logic network is duplicated for Trip Breaker No. 2 using DC power feed No. 2 and the contacts from the "D" relays. Therefore, the two redundant reactor trip logic channels will be physically separated and electrically isolated from one another. Overall, the protection system is comprised of identifiable channels which are physically, electrically and functionally separated and isolated from one another.

Physical Separation

The physical arrangement of all elements associated with the protective system reduces the probability of a single physical event impairing the vital functions of the system.

System equipment is distributed between instrument cabinets so as to reduce the probability of damage to the total systems by some single event.

Wiring between vital elements of the system outside of equipment housing was routed and protected so as to maintain the true redundancy of the systems with respect to physical hazards. The same channel isolation and separation criteria as described for the reactor protection circuits were applied to the engineered safety features actuation circuits.

Loss Power

A loss of power in the Reactor Protective System causes the affected channel to trip. All bistables operate in a normally energized state and go to a de-energized state to initiate action. Loss of power, thus, automatically forces the bistables into the tripped state.

Availability of power to the engineered safety features instrumentation is continuously indicated. The loss of instrument power to the sensors in the engineered safety feature instrumentation starts the engineered safety features equipment associated with the affected channels, except for containment spray which requires instrument power for actuation. Steam line isolation on high-high containment pressure, which utilizes the same actuation circuitry as the containment spray actuation, also requires power to actuate. There are a total of six high-high containment pressure instruments which are separated into three instrument channels. The three high-high containment pressure instrument channels are powered form three separate, independent sources to assure operation in the event of a power failure to one of the instrument channels.

Engineered Safety Features Systems Testing

At least once per 24 months, the master relays will be operated with test input to actuate the safeguards sequences. The test will be terminated upon verification that the associated valves are properly aligned and associated pumps are started by the automatic actuation circuits. No flow is introduced into the Reactor Coolant System; verification of pump startup is by breaker position indication and visual inspection of local flow meters in the mini-flow lines, where applicable. The tests will be performed in accordance with the Technical Specification.

Process Analog Protection Channel Testing

The basic arrangement of elements comprising a representative analog protection channel is shown in Figure 7.2-7. These elements include a sensor or transmitter, power supply, bistable, bistable trip switch and proving lamp, test-operate switch, test annunciator, test signal injection jack, and test points. A portion of the logic system is also included to illustrate the overlap between the typical analog channel and the corresponding logic circuits. The analog system symbols are given in Figure 7.2-14.

Each protection rack include a test panel containing those switches, test jacks and related equipment needed to test the channels contained in the rack. An interlocked hinged cover encloses the test panel. Opening the cover or placing the test-operate switch in the "TEST" position automatically initiates an alarm. These alarms are arranged in rack "sets" to annunciate entry to more than one rack or redundant protection "sets" or channels at any time. The test panel cover is designed such that it cannot be closed (and the alarm cleared) unless the test signal plugs (described below) are removed. Closing the test panel cover mechanically returns the test switches to the "OPERATE" position.

Test procedures allow the bistable output relays of the channel under test to be placed in the tripped mode prior to proceeding with the analog channel tests. Thus, for the channel under test, the relay elements in the two-out-of-three or the two-out-of-four coincident matrices will be in the tripped mode during the entire test of the channel. This ensures that the remaining channels of the two-out-of-three or the two-out-of-four protective functions meet the single failure criterion during the entire channel test. Placing the bistable trip switch in the tripped mode de-energizes (trips) the bistable output relays and connects a proving lamp to the bistable output circuit. This permits the electrical operation of the solid-state bistable to be observed and the bistable set point relative to the channel analog signal to be verified. Test procedures also allow the bistable output relays of the channel under test to be placed in the bypassed mode

prior to proceeding with the analog channel test; i.e., a two-out-of-three circuit becomes a two-out-of-two circuit. Testing in bypass mode is depicted in Figures 7.2-20, 7.2-21, and 7.2-22. This may only be done for circuits whose hardware does not require the use of jumpers or lifted leads to be placed in the bypass mode. Upon completion of test of the analog channel, the bistable trip switches must be manually reset to their operate mode. Closing the cover of the test panel will not transfer the bistable trip switches from their tripped to their operate position.

The following circuits are equipped with trip bypass capability:

| REACTOR TRIP | AUTO SAFETY INJECTION ACTUATION |
|---|---|
| Overpower Delta T | Hi Containment Pressure |
| Over Temperature Delta T | Steam Line Delta P |
| Lo Steam Generator Level | Hi Steam Flow SI |
| Lo-Lo Steam Generator Level | Lo Steam Line Pressure |
| Steam Flow > Feedwater Flow Mismatch | Lo Tavg |
| Pressurizer Hi Pressure | Lo Pressurizer Pressure |
| Pressurizer Lo Pressure | |
| Pressurizer Hi Level | **TURBINE TRIP** |
| Lo Reactor Coolant Flow | Steam Generator Hi-Hi Level |
| Stop Rod Withdrawal | |

Analog channel tests are accomplished by simulating a process measurement signal, varying the simulated signal over the signal span and checking the correlation of bistable set points, channel readouts and other loop elements with precision portable read-out equipment. Test jacks are provided in the test panel for injection of the simulated process signal into each process analog protection channel. Test points are provided in the channel to facilitate an independent means for precision measurement and correlation of the test signal. This procedure does not require any tools nor does it involve in any way the removal or disconnection of wires in the channel under test. In general, the analog channel circuits are arranged so that the channel power supply is loaded and is providing sensing circuit power during channel test. Load capability of the channel power supply is thereby verified by the channel test.

Nuclear Instrumentation Channel Testing

Nuclear Instrumentation Channel Systems (NIS) channels are tested by superimposing the test signal on the actual detector signal being received by the channel. The output of the bistable is not placed in a tripped condition prior to testing. A valid trip signal would then be added to the existing test signal, and thereby cause channel trip at a somewhat lower percent of actual reactor power. Protection bistable operation is tested by increasing the test signal (level signal) to the bistable trip level and verifying operation at control board alarms and/or at the NIS racks.

A NIS channel which can cause a reactor trip through one-out-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. The power range channels do not require bypass of the reactor trip function for test purposes since the protection logic is two-out-of-four. The power range dropped rod function is operated from a one-out-of-four protection logic; therefore, a bypass function is provided on each of the power range channels to prevent load cutback during the dropped rod channel test. Over-riding the dropped rod circuitry from causing a spurious turbine runback due to instrument bus noise has

no impact on the utilization of the Rod Drop Bypass Switch on each Power Range Nuclear Instrument for nuclear instrument testing.

In all cases the bypass condition and the channel test condition are alarmed on the NIS drawer and at the main control board. An interlock feature between the bypass switch and channel test switch on each channel keeps the test signal from being activated until the bypass function has been inserted. Administrative control is required to ensure that only one protection channel is placed in the bypass condition at any one time. The power range reactor trips are not affected by the bypass function described above. Therefore these power range trips will be active if required. No provision was made in the channel test circuit for reducing the channel signal level below that signal being received from the NIS detector.

Logic Channel Testing

The general design features of the logic system are described below. The trip logic channels for a typical two-out-of-three and a two-out-of-four trip function are shown in Figure 7.2-8. The analog portions of these channels are shown in Figure 7.2-9. Each bistable drives two relays ("A & B" for level and "C" & "D" for pressure). Contacts from the "A" and "C" relays are arranged in a 2/3 and 2/4 trip matrix for Trip Breaker No. 1 (RTB). The above configuration is duplicated for Trip Breaker No 2 (RTA) using contacts from the "B" and "D" relays. A series configuration is used for the trip breakers since they are actuated (opened) by undervoltage coils. This approach is consistent with a de-energize-to-trip preferred failure mode. The planned logic system testing includes exercising the reactor trip breakers to demonstrate system integrity. Bypass breakers are provided for this purpose. During normal operation, these bypass breakers are open. Administrative control is used to minimize the amount of time these breakers are closed. Closure of the breaker is controlled from its respective logic test panel in the Control Room. An interlock is provided that trips both bypass breakers open if a second bypass breaker is closed. The status of the breaker is indicated in the Control Room by indicating lights.

As shown in Figure 7.2-8 the trip signal from the logic network is simultaneously applied to the main trip breaker associated with the specific logic chain as well as the Bypass Breaker associated with the alternate trip breaker. Should a valid trip signal occur while Bypass Breaker No. 1 (BYB) is bypassing Trip Breaker No. 1 (RTB), Trip Breaker No. 2 (RTA) will be opened through its associated logic train. The trip signal applied to Trip Breaker No. 2 (RTA) is simultaneously applied to bypass breaker No. 1 (BYB) thereby opening the bypass around Trip Breaker No. 1 (RTB). RTB would either be opened manually as part of the test or would be opened through its associated logic train which would be operational or tripped during a test. Two auxiliary relays are located in parallel with the undervoltage coils of the trip breaker. The output contacts (normally closed) of these relays are connected in series and initiate actuation of the shunt trip coil of both the reactor trip and the associated bypass breaker upon a reactor trip signal. The above contacts are connected to the respective breaker shunt trip coil circuit through test switches which, during the testing of the undervoltage trip device, block the undervoltage trip signal. The test switches are supervised by control room annunciation. In addition, key operated test switches are provided for each train to allow energization of breaker shunt trip coil independent of the undervoltage trip device. The two sets of test switches in conjunction permits selection of particular reactor or bypass breaker to be tested. During response time testing, the shunt trip relay is tied to a portable recorder which is used to indicate transmission of a trip signal through the logic network. Lights are also provided to indicate the status of the individual logic relays.

The following procedure illustrates the method used for testing Trip Breaker No. 1 (RTB) and its associated logic network:

a) Manually set and trip Bypass Breaker No. 1 (BYB) to verify operation.

b) Set BYB; trip Trip Breaker No. 1 (RTB).

c) Place key operated switch "Train-Auto Defeat" to test position, verify alarm and test lamp illumination.

d) Sequentially de-energize the trip relays 9A1, A2, A3) for each logic combination (1-2, 1-3, 2-3). Verify that the logic network de-energizes the UV coil on Trip Breaker No. 1 (RTB) for each logic combination. Since the neon light monitors the signal applied to the UV coil, operation of the UV coil can be determined from the neon light.

e) Repeat "D" for every logic combination in each matrix.

f) Reset Trip Breaker No. 1 (RTB).

g) Trip RTB to validate prior test results as evidenced by the neon light.

h) Reset Trip Breaker No. 1 (RTB). Trip BYB.

In order to minimize the possibility of operational errors from either the standpoint of tripping the reactor inadvertently or only partially checking all logic combinations, each logic network includes a logic channel test panel. This panel includes those switches, indicators and recorders needed to perform the logic system test. The front panel arrangement is shown in Figure 7.2-10. The test switches used to de-energize the trip bistable relays operate through interposing relays as shown in Figures 7.2-7 and 7.2-9. This approach avoids violating the separation philosophy used in the analog channel design. Thus, although test switches for redundant channels are conveniently grouped on a single panel to facilitate testing, physical and electrical isolation of redundant protection channels are maintained by the inclusion of the interposing relay which is actuated by the logic test switches.

If the logic test switches in both engineered safeguards logic trains are placed in the test mode simultaneously, the automatic safeguards actuation will be blocked for the two trains. However, a separate alarm on the main control board is provided for each safeguard train to indicate when each train is in test.

The test switches are located in separate safeguards racks and administrative control prevents the simultaneous operation of Train A and Train B test switches.

It should be noted that either one of the safeguards train, which is blocked by its test switch, can always be unblocked and actuated by the manual safety injection switch at the main control board.

Safeguards Initiating Circuitry

The safeguards actuation circuitry and hardware layout are designed to maintain circuit isolation through the bistable operated logic relays. The channelized design follow through is shown on the Figure 7.2-15 block diagram.

The orderly arrangement of equipment for the Reactor Protection System and Engineered Safety Features Actuation System helps facilitate testing and maintenance. A color code of red, white, blue and yellow is used for analog protection channels in sets I, II, III, and IV, respectively. Large identification plates with the appropriate background color are attached at the front and back surfaces of each analog rack. The protection logic cabinets, housing the Train A logic, master relays, and slave relays, are physically separated from cabinets housing Train B equipment and identified by large identification plates on the input side of the racks where protection signals from the various protection channels are received. Small electrical components have nameplates on the enclosure which houses them. All cables are numbered with identification tags. These numbers are cross-referenced with cable schedule which specifies cable routing and function. The cable trays are color coded with each of the four channels having a different color assigned.

The safeguards bistables, mounted in the analog protection racks, drive both "A" and "B" logic matrix relays. Each matrix contains its own test light and test circuitry. The "A" and "B" logic matrices operate master relays for actuating channels A and B respectively, as shown in Figure 7.2-16.

Control power for logic channels A and B, is supplied from DC distribution panel No. 31 and No. 34, respectively. These redundant actuating channels operate the various safeguards components required with the large loads sequenced as necessary.

Protection channel identity is lost in the intermixing of the relay matrix wiring. Separation of A and B logic channels is maintained by the separate logic racks.

For safety injection, manual reset of the safeguards actuation relays may be accomplished two minutes following their operation. Once reset action is taken, the master relay is reset and its operation blocked, except for manual initiation. The engineered safeguards circuitry can be unblocked by resetting the reactor trip breaker.

Hinged safety covers on the reset pushbuttons in the circuitry of the Safety Injection, Containment Spray, Containment Isolation Phase A and Phase B, and Containment Ventilation Isolation Systems require deliberate action by the operators to actuate these pushbuttons and facilitate placing adequate administrative controls on the actuation of these pushbuttons. The Containment Ventilation Isolation System cannot be placed in a bypass condition while any of the automatic safety signals is present.

Separate and independent key-lock switches, one for each SI train, are provided in series to each of the auto SI actuation relays to allow manual blocking of the Engineered Safeguards System actuation. (See Section 6.2.2)

Logic Channel Testing

Figures 7.2-16 and 7.2-17 show the basic logic test scheme. Test switches are located in associated relay racks rather than in a single test panel. The following procedure is used for testing the logic matrices:

1) Following administrative procedure, test Channel A or B, one at a time

2) Depress the test relay switch to energize the rack test relays. An alarm will sound on the main board and a light at the rack will indicate that the safeguards rack is now in test.

3) Select a matrix and depress the logic test switches. The master relay will energize and matrix test lights will indicate upon actuation of the particular matrix being tested. The slave relay test lights will verify that the master relay contact associated with a particular slave relay has functioned and will also verify the integrity of the slave relay coils.

4) Reset the master relay by depressing the master relay reset switch. Reset the test relays by depressing the test reset switch. A lamp will glow as long as the test relays are energized. If a test relay contact in a particular slave relay circuit does not return to its normal position, then the slave relay test lamps will indicate such. Test lights can be tested by depressing the lens.

Primary Power Source

The primary source of control power for the Reactor Protective System is the vital instrument buses described in Chapter 8. The source of power for the measuring elements and the actuation circuits in the engineered safety features instrumentation is also from those buses.

Protective Actions

Reactor Trip Description

The Reactor Protection System acts to shut the reactor down by means of various reactor trips which are designed to occur when a measured plant variable exceeds predetermined limits. The protection system consists of all instrumentation which monitors the process variables and initiates trip if the process variables approach safety limits. It includes, but is not limited to, sensing elements, transmitters, converters, relays, actuating devices, interlocks, alarms, signal lines, etc. The trips function to provide rapid reduction of reactivity by the insertion of full-length RCC assemblies under free fall into the reactor core. The full-length RCC assemblies must be energized to remain withdrawn from the core.

Automatic reactor trip occurs upon the loss of power to the full-length control rods. All power to the full-length control rod mechanisms are interlocked by duplicate series connected circuit breakers. The trip breakers are opened by the undervoltage coils on both breakers. The undervoltage coils, which are normally energized, become de-energized by any one of the several trip signals.

Certain reactor trip channels (low reactor coolant flow, etc.) are automatically bypassed at low power where they are not required for safety. Nuclear source range, intermediate range and power range (low setpoint) trips, which are specifically provided for protection at low power or subcritical operation, are bypassed by operator manual action after receiving a permissive signal from the next higher range of instrumentation to allow power escalation during startup.

During power operation, a sufficiently rapid shutdown capability in the form of RCC assemblies is administratively maintained through the control rod insertion limit monitors. Administrative control requires that all shutdown rods be in the fully withdrawn position during power operation.

A resume of reactor trips, including means of actuation and the coincident circuit requirements, is given in Table 7.2.1. The permissive circuits referred to (e.g., P-7) are listed in Table 7.2-2.

Manual Trip

The manual actuating devices are independent of the automatic trip circuitry and are not subject to failures which might make the automatic circuitry inoperable. Either of two manual trip devices located in the Control Room will initiate a reactor trip.

High Nuclear Flux (Power Range) Trip

This circuit trips the reactor when two of the four power range channels read above the trip setpoint. There are two independent trip settings, one high and one low setting. The high trip setting provides protection during normal power operation. The low setting, which provides protection during startup, can be manually bypassed when two out of the four power range channels read above approximately 10% power (P-10). Three out of the four channels below 10% automatically reinstates the trip protection. The high setting is always active.

High Nuclear Flux (Intermediate Range )Trip

This circuit trips the reactor when one out of the two intermediate range channels reads above the trip setpoint. This trip, which provides protection during reactor startup, can be manually bypassed if two out of four power range channels are above approximately 10% (P-10). Three out of four channels below this value automatically reinstate the trip protection. The intermediate channels (including detectors) are separate from the power range channels.

High Nuclear Flux (Source Range) Trip

This circuit trips the reactor when one of the two source range channels reads above the trip setpoint. The trip, which provides protection during reactor startup, can be manually bypassed when one of two intermediate range channels reads above the P-6 setpoint value and is automatically reinstated when both intermediate range channels decrease below this value (P-6). This trip is also bypassed by two out of four high power range signals (P-10). It can also be reinstated below P-10 by an administrative action requiring coincident manual actuation.

The trip point is set between the intermediate range lower limit of instrument sensitivity and the upper limit of the source range instrument range.

Overtemperature ΔT Trip

The purpose of this trip is to protect the core against DNB. This circuit trips the reactor on coincidence of two-out-of-the-four signals with one channel (two temperature measurement, hot and cold) per loop. The set point for this reactor trip is continuously calculated for each channel by solving equations of this form:

$$\Delta T_{trip} - \Delta T_o [K_1 - K_2 (T_{avg} - T') + K_3 (P - P') - f (\Delta I)]$$

where

$\Delta T_o$ - indicated ΔT at rated power, F

$T_{avg}$ - reactor coolant average temperature, two measurements in each loop ($T_{avg}$ signal is rate compensated), F

T' - indicated $T_{avg}$ at nominal condition at rated power, F

P - pressurizer pressure, four independent measurements, psia

P' - nominal pressure at rated power, psia

$K_1$ - set point bias, F

$K_2$, $K_3$ - constants based on the effect of temperature and pressure on the DNB limits

f (ΔI) - a function of the indicated difference between top and bottom detectors of the power range nuclear ion chambers with gains selected based on measured instrument response during plant startup tests.

Overpower ΔT Trip

The purpose of this trip is to protect against excessive power (fuel rod rating protection). This circuit trips the reactor on coincidence of two out of the four signals with one channel (one pair of temperature measurements) per loop.

The set point for this reactor trip is continuously calculated for each channel by solving equations of the form;

$$\Delta T_{set\ point} - \Delta T_o \left[K_4 - K_5 \frac{dT_{avg}}{dt} - K_6 (T_{avg} - T')\right]$$

where

$\Delta T_o$ - indicated ΔT at rated power, F

$T_{avg}$ - Average temperature, F

T' - Indicated $T_{avg}$ at nominal conditions at rated power, F

$K_4$ - Set point bias

$K_5$ - Constant

$K_6$ - Constant

Low Pressurizer Pressure Trip

The purpose of this circuit is to protect against excessive core steam voids which could lead to DNB. The circuit trips the reactor on coincidence of two out of the four low pressurizer pressure signals. This trip is blocked when any three of the four power range channels and two of two turbine first stage (inlet) pressure channels read below approximately 10% power (P-7).

High Pressurizer Pressure Trip

The purpose of this circuit is to limit the range of required protection from the overtemperature ΔT trip and to protect against Reactor Coolant System over-pressure. This circuit trips the reactor on coincidence of two out of the three high pressurizer pressure signals.

High Pressurizer Water Level Trip

This trip is provided as a backup to the high pressurizer pressure trip. The coincidence of two out of the three high pressurizer water level signals trips the reactor. The trip is bypassed when any three of the four power range channels and two of the two turbine first stage (inlet) pressure channels read below approximately 10% power (P-7).

Low Reactor Coolant Flow Trip

The trip protects the core form DNB following a loss of coolant flow accident. The means of actuating the loss of coolant flow accident trip are:

a) Measured low flow in the reactor coolant loop. The low flow trip signal is actuated by the coincidence of 2/3 signals of any reactor coolant loop. The loss of flow in any two loops causes a reactor trip above approximately 10% power (P-7). Above the P-8 setpoint any one loop causes a reactor trip. The sensor used for flow measurement is an elbow tap and is discussed in Chapter 4.

b) Reactor coolant pump circuit breaker open functions similarly to the low flow signal with one sensor per reactor coolant pump breaker.

c) Underfrequency on any two of the four reactor coolant pump buses will trip all four reactor coolant pumps and cause a reactor trip above approximately 10% power (P-7).

d) Undervoltage on any two of the four reactor coolant pump buses causes a direct reactor trip above approximately 10% power (P-7).

Safety Injection System (SIS) Actuation Trip

A reactor trip occurs when the Safety Injection System is actuated. The means of actuating the SIS trips are:

1) Low pressurizer pressure (two out of three). This signal may be manually blocked or unblocked during start-up and shutdown. This block is accomplished by separate switches for each of the redundant safety injection initiation circuits. The block will be automatically removed above a designated setpoint.

2) High containment pressure (two out of three) set at approximately 10% of containment design pressure.

3) High differential pressure between any two steam lines (two out of three).

4) After time delay: high steam flow in 2/4 lines (one out of two per line), in coincidence with either low $T_{avg}$ in 2/4 lines or low steam line pressure in 2/4 lines.

5) High-high containment pressure (two sets of two-out-of-three), set at approximately 50% of containment design pressure [energize to actuate].

6) Manual.

Turbine Generator Trip

A turbine trip is sensed by two out of three signals from auto-stop oil pressure. A turbine trip is accompanied by a direct reactor trip above P-8 and a controlled short term release of steam to the condenser occurs which removes sensible heat from the Reactor Coolant System while avoiding steam generator safety valve actuation. Any reactor trip will generate a turbine trip. Further details are discussed in Chapter 10.

Steam/Feedwater Flow Mismatch Trip

This trip protects the reactor from a sudden loss of heat sink. The trip is actuated by one steam/feedwater flow mismatch in selected coincidence with one low steam generator water level in that steam generator. There are two steam/feedwater flow mismatches and two low steam generator water level signals per loop.

Low-Low Steam Generator Water Level Trip

The purpose of this trip is to protect the steam generators for the case of a sustained steam/feedwater flow mismatch. The trip is actuated on two out of the three low-low water level signals in any steam generator. A diagram of the steam generator level control and protection system is shown in Plant Drawing IP3V-0171-0355 [Formerly Figure 7.2-13].

Rod Stops

A list of rod stops is listed in Table 7.2-3. Some of these have been previously noted under permissive circuits, but are listed again for completeness.

Rod Drop Protection

Two independent systems are provided to sense a dropped rod: a rod bottom position detection system and a system which senses sudden reduction in out-of-core neutron flux. Both protection systems initiate protective action in the form of blocking automatic rod withdrawal, and also, a turbine load cutback if above a given power level. This action compensates for accessible adverse core power distributions and permits an orderly retrieval of the dropped RCC.

The primary protection for the dropped RCC accident is the rod bottom signal derived for each rod from its individual position indication system. With the position indication system, initiation of protection is independent of rod location of reactivity worth.

Backup protection is provided by use of the out-of-core power range nuclear detectors and is particularly effective for large nuclear flux reductions occurring in the region of the core adjacent to the detectors.

The rod drop detection circuit from nuclear flux consists basically of a comparison of each ion chamber signal with the same signal taken through a first order lag network. Since a dropped

RCC assembly will rapidly depress the local neutron flux, the decrease in flux will be detected by one or more of these four sensors. Such a sudden decrease in ion chamber current will be seen as a difference signal. A negative signal output greater than a preset value (approximately 10%) from any of the four power range channels will actuate the rod drop protection.

Figure 7.4-2 indicates schematically the dropped rod detection circuits and the Nuclear Protection System in general. The potential consequences of any dropped RCC without protective action are presented in Section 14.1.4.

Alarms

Any of the following conditions actuate an alarm:

a) Reactor trip (first-out annunciator)

b) Trip of any reactor trip channel

c) Significant deviation of any major control variable (pressure, $T_{avg}$, pressurizer water level, and steam generator water level)

d) Actuation of any permissive circuit or override. (Certain permissive are provided with indication light only on the flight panel.)

Control Group Rod Insertion Limits

The control rod insertion limit system is used in an administrative control procedure with the objective to maintain an RCCA shutdown margin.

The control group rod insertion limits, $Z_{LL}$, are calculated as a linear function of reactor power and reactor coolant average temperature. The equation is:

$$Z_{LL} - A\,(\Delta T)_{avg} + B\,(\overline{T_{avg}}) + C$$

where A and B are preset manually adjustable gains and C is a preset manually adjustable bias. These set points may be different for each control bank. The $(\Delta T)_{avg}$ and $(\overline{T_{avg}})$ are the average of the individual temperature differences and the coolant average temperatures, respectively, measured from the reactor coolant hot leg and cold leg.

One insertion limit monitor with two alarm set points is provided for each control bank. A description of control and shutdown rod groups is provided in Section 7.3. The low alarm alerts the operator of an approach to a reduced shutdown reactivity situation requiring boron addition by following normal procedures with the Chemical and Volume Control System (Chapter 9). Actuation of low-low alarm requires the operator to take immediate action to add boron to the system by any one of several alternate methods.

7.2.3 System Evaluation

Reactor Protection System and DNB

The following is a description of how the reactor protection system prevents DNB.

The plant variables affecting the DNB ratio are:
- Thermal power
- Coolant flow
- Coolant temperature
- Coolant pressure
- Distribution Core power (hot channel factors)

Figure 7.2-11 illustrates the core limits for which DNBR for the hottest rod is at the design limit and shows the overpower and overtemperature ΔT reactor trips locus as a function of $T_{avg}$ and pressure.

Excessive axial offset reduces the overtemperature ΔT setpoint associated with both the block on control rod withdrawal and the reactor trip actuation. If the ΔT of any RCS loop exceeds the calculated overpower or overtemperature ΔT setpoints, permissive signals will be generated which will initiate a block on control rod withdrawal. The setpoint on these ΔT rod blocks are approximately 2° F less than the corresponding ΔT setpoints used to actuate reactor tip. This provides a margin or buffer prior to achieving operating conditions requiring a reactor trip on overpower or overtemperature. Rod block on ΔT circuitry is not redundant, whereas the ΔT reactor trips are protective grade and meet the standards of IEEE-279.

Reactor trips for a fixed high pressurizer pressure and for a fixed low pressurizer pressure are provided to limit the pressure range over which core protection depends on the variable overpower and overtemperature ΔT trips.

Reactor trips on nuclear overpower and low reactor coolant flow are provided for direct, immediate protection against rapid changes in these variables. However, for all cases in which the calculated DNBR approaches the applicable DNBR limit, a reactor trip on overpower and/or overtemperature ΔT would be actuated.

The ΔT trip functions are based on the differences between measurements of the hot leg and cold leg temperatures, which are proportional to core power.

The overtemperature ΔT trip function is provided with a nuclear flux feedback to reflect a measure of axial power distribution. This will assist in preventing an adverse distribution which could lead to exceeding allowable core conditions.

Overpower Protection

In addition to the high power range nuclear flux trips, an overpower ΔT trip is provided (2 out of 4 logic) to limit the maximum overpower.

A rod stop function and turbine runback function is provided in the form:

$\Delta^T$ rod stop = $\Delta^T$ trip - $B_p$

$B_P$ = set point bias (F)

The logic for the runback is one out of four.

Overtemperature Protection

A second $\Delta T$ trip (2 out of 4 logic) provides an overtemperature trip which is a function of coolant average temperature and pressurizer pressure derived as previously discussed.

A similar rod stop function is provided in the form;

$\Delta^T$ rod stop = $\Delta^T$trip $^{-B}T$

$^BT$ = set point bias, F

The logic for the rod stop is one out of four.

In summary, in the event the difference between top and bottom detectors exceeds the desired range, automatic feedback signals are provided to reduce the overtemperature trip setpoint and to block rod withdrawal to maintain appropriate operating margins to the trip setpoint.

Interaction of Control and Protection

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

Specific Control and Protection Interactions

Nuclear Flux

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

In addition, the control system will respond only to rapid changes in indicated nuclear flux; slow changes or drifts are overridden by the temperature control signals. Also, a rapid decrease of any nuclear flux signal will block automatic rod withdrawal as part of the rod drop protection circuitry.

Finally, an overpower signal from any nuclear channel will block automatic rod withdrawal. The set point for this rod stop is below the reactor trip set point.

Coolant Temperature

Four $T_{avg}$ channels are used for overtemperature-overpower protection. (See Plant Drawings IP3V-0171-0052, -0053, -0054, and -0055 [Formerly Figure 7.2-12] for single channel). Isolated output signals from all four channels are also averaged for automatic control rod regulation. In principle, a spuriously low temperature signal from one sensor could cause rod withdrawal and overtemperature. Two-out-of-four overtemperature and overpower ΔT logic will ensure a trip is needed even with an independent failure in another channel. In addition, channel deviation alarms in the control system will block automatic rod withdrawal if any temperature channel deviates significantly from the others. Automatic rod withdrawal blocks will also occur if any one of four nuclear channels indicates an overpower condition or if any one of the four temperature channels indicates an overtemperature condition. Finally, as shown in Section 14.1, the combination of trips on nuclear overpower, high pressurizer water level, and high pressurizer pressure also serve to limit an excursion for any rate of reactivity insertion.

Narrow range RCS hot leg temperature is measured for each channel through the use of three RTDs located 120° apart. The three RTD signals are averaged by a microsprocessor to produce the hot leg signal for the channel. The microprocessor has the capability to detect a failure of any of the hot leg RTDs.

Pressurizer Pressure

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

1) Pressure Control. Spray, power-operated relief valves, and heaters are controlled by isolated output signals from the pressure protection channels:

   a) Low Pressure

      A spurious high pressure signal from one channel can cause low pressure by actuation of a pressurizer spray valve. Spray reduces pressure at a low rate, and some time is available for operator action (about three minutes at maximum spray rate) before a low pressure trip is reached. Additional redundancy is provided by the protection system to ensure underpressure protection, i.e., two-out-of-four low pressure reactor trip logic and two-out-of-three safety injection logic.

      Each pressurizer relief valve is interlocked to prevent opening on a single high pressure signal. Furthermore, the valve setpoint is at a higher pressure than the normal high pressure signal actuation pressure.

   b) High Pressure

      The pressurizer heaters are incapable of overpressurizing the Reactor Coolant System. Maximum steam generation rate with heaters is about 15,000 lbs/hr, compared with a total capacity of 1,260,000 lbs/hr for the three safety valves and total capacity of 358,000 lbs/hr of the two power-operated relief valves. Therefore, overpressure protection is not required for a pressure control failure. Two-out-of-three high pressure trip logic is therefore used.

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

An Overpressure Protection System prevents the reactor vessel pressure from exceeding the Technical Specification limits, as described in Section 4.3.4.

c) Pressurizer Level

The presssurizer level channels are used for high level reactor trip two out of three. Isolated output signals from these channels are used for volume control, increasing or decreasing water level. A level control failure could fill or empty the pressurizer at a slow rate (on the order of half an hour or more).

2) High Level

A reactor trip on pressurizer high water level is provided to prevent rapid thermal expansions of reactor coolant fluid from filling the pressurizer; the rapid change from high rates of steam relief to water relief can be damaging to the safety valves and relief piping and pressure relief tank. However, a level control failure cannot actuate the safety valves because the high pressure reactor trip is set below the safety valve set pressures. Therefore, a control failure does not require protection system action. In addition, ample time and alarms are available for operator action.

3) Low Level

For control failures which tend to empty the pressurizer, a low level signal from either of two independent level control channels will isolate letdown, thus preventing the loss of coolant. Ample time and alarms exist for operator action.

A low pressurizer level will result for all Loss-of-Coolant Accidents except for a special class of breaks in the range of 2 to 6 inches which occur in the vapor space of the pressurizer. For this special class which does not result in low pressurizer water level, the reactor will be tripped on either low pressure or DT overtemperature as the pressure drops, and DNB will be prevented. Following reactor trip, there will be no core damage as long as the core remains covered. Sufficient time is available in accidents of this type for the operator to take manual control of makeup to assure core cooling during subsequent cold shutdown procedures.

Sufficient redundancy is provided to accommodate the loss of one level channel without jeopardizing functional capability of the reactor protection system. In the Technical Specifications, limits are set on the minimum number of operable channels and required plant status for all reactor protection instrumentation.

Steam Generator Water Level; Feedwater Flow

Before describing control and protection interaction for these channels, it is beneficial to review the protection system basis for this instrumentation.

The basic function of the reactor protection circuits associated with low steam generator water level and low feed water flow is to preserve the steam generator heat sink for removal of long term residual heat. Should a complete loss of feedwater occur with no protective action, the steam generators would boil dry and cause an overtemperature-overpressure excursion in the reactor coolant. Reactor trips on temperature, pressure, and pressurizer water level will trip the plant before there is any damage to the core or reactor coolant system. However, residual heat generated after the reactor trip would cause a pressure spike in the pressurizer that lifts the pressurizer relief valves and causes discharge of liquid reactor coolant to the Containment. Redundant auxiliary feedwater pumps are provided to prevent this. Reactor trips act before the steam generators are dry to reduce the required capacity and starting time requirements of these pumps and to minimize the thermal transient on the reactor coolant system and steam generators. Independent trip circuits are provided for each steam generator for the following reasons:

1) Should severe mechanical damage occur to the feedwater line to one steam generator, it is difficult to ensure the functional integrity of level and flow instrumentation for that unit. For instance, a major pipe break between the feedwater flow element and the steam generator would cause high flow through the flow element. The rapid depressurization of the steam generator would drastically affect the relation between downcomer water level and steam generator water inventory.

2) It is desirable to minimize thermal transient on a steam generator for credible loss of feed water accidents.

   It should be noted that controller malfunctions caused by a protection system failure affect only one steam generator. Also, they do not impair the capability of the main feedwater system under either manual control or automatic Tavg control. Hence, these failures are far from being the worst case with respect to decay heat removal with the steam generators.

   a) <u>Feedwater Flow</u>

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

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

   b) <u>Steam Flow</u>

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

   c) <u>Level</u>

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

1) A rapid increase in the level signal will completely stop feedwater flow and actuate a reactor trip on low feedwater flow coincident with low level.

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

7.2.4 Qualification Testing

Typical protection system equipment is subjected to type tests under simulated seismic acceleration to demonstrate its ability to perform its functions. Type testing is performed using conservatively large accelerations and applicable frequencies. The peak accelerations and frequencies used are checked against those derived by structural analysis of operational and design basis earthquake loadings. Typical switches and indicators for safety features components have been tested to determine their ability to withstand seismic forces without malfunction which would defeat automatic operation of the required component.

For testing there is no adequate way of knowing what combination of vertical and horizontal input motion produces the worst effects (e.g., stresses, deflections). There is a greater probability that due to the phase relationship of the two simultaneously applied input motions, the resulting combined motion produces less severe effects than when these motions are applied separately. Testing in one direction at a time is considered the best way to obtain positive proof of the equipment's capability. (The independent testing in each of the three directions is also recommended in the IEEE Guide for Seismic Qualifications of Class I Electric Equipment.) Furthermore, the uni-directional testing was performed in a conservative manner, thus providing a margin against any greater effects which may possibly result from the worst combination of simultaneous testing. These conservatisms consist of: (1) an input sine beat motion with 10 cycles per beat, (2) resonant testing at all determined and applicable natural frequencies, (3) further testing at other selected frequencies, and (4) high input acceleration values, particularly for the vertical direction.

Qualification testing was performed on various safety systems such as process instrumentation and nuclear instrumentation. This testing involved demonstrating operation of safety functions at elevated ambient temperatures to 120°F for original control room equipment.

To establish the combined effect upon protection systems of long term operation followed by exposure to accident conditions inside the containment, selected components were subjected to thermal aging followed by irradiation. In addition, components were first irradiated and then subjected to thermal aging. Results of the tests indicate that the components would perform satisfactorily following a Design Basis Accident.

Cables of the type used for Indian Point 3 were tested using the same approach as described above, i.e., irradiation, thermal aging followed by steam exposure and thermal age, and irradiation followed by steam exposure. During exposure to steam, the cables carry nominal voltage and current.

Westinghouse Topical Reports, WCAP-7817[1], WCAP-7817 Supplement 1[2], and WCAP-8234[3] provide the seismic evaluation of safety related equipment. The type tests covered by these reports are applicable to Indian Point 3.

## References

1) Vogeding, E. L., "Seismic Testing of Electrical and Control Equipment," WCAP-7817, December 1971.

2) Vogeding, E. L., "Seismic Testing of Electrical and Control Equipment (WCID Process Control Equipment)," WCAP-7817 Supplement 1, December 1971.

3) "Seismic Testing and Functional Verification of By-Pass Loop Reactor Coolant RTD's," WCAP-8234 (Westinghouse Non-Proprietary Class 3), June 1974.

4) NSE 94-3-124 ED, Rev. O "Evaluation of Cable Channelization Deficiencies."

Table 7.2-1

LIST OF REACTOR TRIPS & CAUSES OF ACTUATION OF:
ENGINEERED SAFETY FEATURES, CONTAINMENT AND STEAM LINE ISOLATION & AUXILIARY FEEDWATER

| | COINCIDENCE CIRCUITRY AND INTERLOCKS | COMMENTS |
|---|---|---|
| REACTOR TRIP | | |
| | | |
| 1) Manual | ½, no interlocks | |
| 2) Overpower nuclear flux | 2/4 | High and low settings; manual block and automatic reset of low setting by P-10, Table 7.2-2 |
| 3) Overtemperature T | 2/4, no interlocks | |
| 4) Overpower T | 2/4, no interlocks | |
| 5) Low pressurizer pressure | 2/4, blocked by P-7 | |
| 6) High pressurizer pressure (fixed set points) | 2/3, no interlocks | |
| 7) High pressurizer water level | 2/3, blocked by P-7 | |
| 8) a. Low reactor coolant flow | 2/3, per loop, blocked by P-7, P-8 | |
| b. Reactor coolant pump breaker | 1/1, per loop, blocked by P-7, P-8 | Reactor coolant pump breaker is tripped on underfrequency |
| c. Undervoltage on reactor coolant pump bus | 2/4, per loop, blocked by P-7 | |
| d. Underfrequency on reactor coolant pump bus | 2/4 | Underfrequency trips all reactor coolant pumps |
| 9) Safety injection signal (Actuation) | 2/3, low pressurizer pressure (manual block permitted by 2/3 low pressurizer pressure): or 2/3 high containment pressure (high-level): or 2/3 high differential pressure between any two steam lines, or manual ½, or two sets of 2/3 hi-hi containment pressure (high-high pressure) [energize to actuate], or after delay (maximum 6 seconds) with high steam flow in 2/4 lines coincidence with (a) low $T_{avg}$ in 2/4 lines or (b) low steam line pressure in 2/4 lines | |
| 10) Turbine generator | 2/3, blocked by P-8 | Low auto-stop oil pressures signal |
| 11) Steam/feedwater flow mismatch | ½ steam/feedwater flow mismatch in selected coincidence with low steam generator water level | |



276

Table 7.2-1

LIST OF REACTOR TRIPS & CAUSES OF ACTUATION OF:
ENGINEERED SAFETY FEATURES, CONTAINMENT AND STEAM LINE ISOLATION & AUXILIARY FEEDWATER

| | COINCIDENCE CIRCUITRY AND INTERLOCKS | COMMENTS |
|---|---|---|
| | in that steam generator | |
| 12) Low-low steam generator water level | 2/3, per loop | |
| 13) High intermediate range nuclear flux | ½, manual block permitted by P-10 | Manual block and automatic reset |
| 14) High source range nuclear flux | ½, manual block permitted by P-6, block maintained by P10 | Manual block and automatic reset of P-6; manual reset of P-10 |
| **CONTAINMENT ISOLATION ACTUATION** | | |
| 15) Safety Injection Signal (Phase A) | See Item 9 | Actuates all non-essential service containment isolation trip valve and actuates Isolation Valve Seal Water System |
| 16) Containment pressure (Phase B) | Coincidence of two sets of 2/3 containment pressure (High-high pressure [energize to actuate], same signal which actuates containment spray), or manual 2/2 | Actuates all essential service containment isolation trip valves |
| 17) Containment ventilation (High containment activity) | ½ high activity signal, from air particulate detector or radiogas detector or containment isolation phase "A" signal, or spray actuation signal | This additional signal closes containment purge supply, exhaust ducts and pressure relief duct only |
| **ENGINEERED SAFETY FEATURES ACTUATION** | | |
| 18) Safety injection signal (S) | See Item 9 | |
| 19) Containment spray signal (P) | Coincidence of two sets of 2/3 containment pressure (high-high pressure); or manual 2/2 (Note: Bistables are energize-to-operate) | |
| 20) Spray additive valves | Coincidence of two sets of 2/3 contaiment pressure (high-high pressure, same signal which actuates containment spray (Note: Bistables are energize-to-operate) | |
| 21) Containment air recirculation cooling and filtration signal | Safety injection signal initiates starting of all fans in accordance with the safety injection starting sequence, 2/3 high containment pressure or manual ½ | |
| 22) Isolation valve seal water signal | Safety injection signal | |

Table 7.2-1

LIST OF REACTOR TRIPS & CAUSES OF ACTUATION OF:
ENGINEERED SAFETY FEATURES, CONTAINMENT AND STEAM LINE ISOLATION & AUXILIARY FEEDWATER

| | COINCIDENCE CIRCUITRY AND INTERLOCKS | COMMENTS |
|---|---|---|
| **STEAM ISOLATION ACTUATION** | | |
| 23) Steam flow | After time delay (maximum 6 seconds) with high steam flow in 2/4 lines in coincidence with (a) low $T_{avg}$ in 2/4 lines or (b) low steam line pressure in 2/4 lines | |
| 24) Containment pressure | Coincidence of two sets of 2/3 Containment pressure (high-high pressure) (Note: Bistables are energize-to-operate) | |
| 25) Manual | 1/1 per steam line | |
| **AUXILIARY FEED WATER ACTUATION** | | |
| 26) Turbine driven pump | Coincidence of 2/3 low level in two steam generators; or a non-SI blackout sequence signal from 480 volt buses 3A or 6A; or manual ½; or AMSAC Actuation | |
| 27) Motor driven pumps | 2/3 low level in any steam generator; or trip of ½ main feedwater pump turbines; or safety injection signal; or manual ½; or a non-SI blackout sequence signal from 480 volt bus 3A to start pump 31; or a non-SI blackout sequence signal from 480 volt bus 6A to start pump 33; or AMSAC Actuation | |
| **MAIN FEEDWATER ISOLATION** | | |
| 28) Close main feedwater control valves, (including associated MOVs) trip main feedwater pumps | Any safety injection signal (See Item 9) | |



298

TABLE 7.2-2

INTERLOCK AND PERMISSIVE CIRCUITS

| Number | Function | Input for Blocking |
|---|---|---|
| 1 + | Prevent rod withdrawal on overpower | ¼ high nuclear flux (power range) or ½ high nuclear flux (intermediate range or ¼ overtemperature ΔT or ¼ overpower ΔT |
| 2 | Auto-rod withdrawal stop at low power | Low MWe load signal |
| 3+ | Auto-rod withdrawal stop on rod drop | ¼ rapid decrease of nuclear flux (power range) or 1/1 rod bottom indication |
| 4* | [BLANK – See Note] | |
| 5 + | Steam dump interlock | Turbine trip signal |
| 6 | Manual block of source range level trip | ½ high intermediate range flux allows manual block, 2/2 low intermediate range defeats block |
| 7 | Permissive power (block various trips required only at power) | ¾ low-low nuclear flux (power range) and 2/2 low turbine impulse chamber pressure signal |
| 8 | Block single primary loop loss of flow trip and Block Reactor Trip on Turbine Trip | ¾ low nuclear flux (power range) |
| 9* | | |
| 10 | Manual block of low setpoint trip (power range) and intermediate range trips | 2/4 high nuclear flux allows manual block, ¾ low nuclear flux (power range) defeats manual block |

NOTE:
* not applicable to this plant
+ alarmed

TABLE 7.2-3

ROD STOPS

| Rod Stop | Actuation Signal | Rod Motion to be blocked |
|---|---|---|
| 1. Rod Drop | ¼ rapid power range nuclear | Automatic Withdrawal |
| | flux decrease or any rod bottom signal | Actuation of rod stop (Item 1) initiates a turbine load reduction above a given power level |
| 2. Nuclear Overpower | ¼ high power range nuclear flux or ½ high intermediate range nuclear flux | Automatic and Manual Withdrawal |
| 3. High ΔT* | ¼ overpower ΔT or ¼ overtemperature ΔT | Automatic and Manual Withdrawal |
| 4. Low Power | Low turbine first stage (inlet) pressure load signals | Automatic Withdrawal |
| 5. $T_{avg}$ Deviation | ¼ $T_{avg}$ deviation from average $T_{avg}$ | Automatic Withdrawal |

*NOTE: Actuation of rod stop (Item 3) initiates a load cutback at any power level.

IP3
FSAR UPDATE

[redacted]

[redacted]

| [redacted] | [redacted] |  | [redacted] | [redacted] | [redacted] | [redacted] |
|---|---|---|---|---|---|---|
| [redacted] |  |  |  |  |  |  |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |

[redacted]

283

284

## 7.3 REGULATING SYSTEMS

### 7.3.1 Design Basis

The Reactor Control System is designed to limit nuclear plant transients for prescribed design load perturbations, under automatic control, within prescribed limits to preclude the possibility of a reactor trip in the course of these transients.

Overall reactivity control is achieved by the combination of chemical shim and 53 control rod clusters of which 29 are in 4 control banks and 24 are in 4 shutdown banks. Long-term regulation of core reactivity is accomplished by adjusting the concentration of boric acid in the reactor coolant. Short-term reactivity control for power changes or reactor trip is accomplished by movement of control rod clusters.

The primary function of the Reactor Control System is to provide automatic control of the rod clusters during power operation of the reactor. The system uses input signals including neutron flux; coolant temperature and pressure; and plant turbine load. The Chemical and Volume Control System (Chapter 9) serves as a secondary reactor control system by the addition and removal of varying amounts of boric acid solution.

There is no provision for a direct continuous visual display of primary coolant boron concentration. When the reactor is critical, the best indication of reactivity status in the core is the position of the control group in relation to plant power and average coolant temperature. There is a direct, predictable, and reproducible relationship between control rod position and power and it is this relationship which establishes the lower insertion limit calculated by the rod insertion limit monitor. There are two alarm setpoints to alert the operator to take corrective action in the event a control bank approaches or reaches its lower limit. Rod position is also a function of core life.

Any unexpected change in the position of the control banks when under automatic control or a change in coolant temperature when under manual control provides a direct and immediate indication of a change in the reactivity status of the reactor. In addition, periodic samples of coolant boron concentration are taken. The variation in concentration during core life provides a further check on the reactivity status of the reactor including core depletion.

The Reactor Control System is designed to enable the reactor to follow load changes automatically when the plant output is above 15% of nominal power. Control rod positioning may be performed automatically when plant output is above this value, and manually at any time.

Overriding the rod stop and turbine runback signals from the Overpower or Overtemperature $\Delta T$ circuitry, or from the Power Range Nuclear Instrument Dropped Rod circuitry has no impact on the prevention of automatic control rod withdrawal below 15% of nominal power. Overriding one channel of these signals has no impact on reactor protection in the event of an approach to an overpower condition in as much as the reactor trips associated with such a condition remains unaffected. Additionally, since only one channel at a time is permitted to be affected, the other three channels remain available for rod stop and turbine runback on either Overpower or Overtemperature $\Delta T$, or on Power Range Nuclear Instrument Rod Drop signals.

The system enables the nuclear plant to accept the following transients without reactor trip subject to possible xenon limitations:

a) Step load increases to 10% within the load range of 15% to 90% of full power

b) Step load reduction of 10% within the load range of 100% to 25% of full power

c) A 5% per minute ramp load change within the load range of 15% to 100% of full power.

The operator is able to select any single bank of rods (shutdown or control) for manual operation. Using a single switch, he may not select more than one bank from these two functions. He may also select automatic reactor control, in which case, the control banks can be moved only in their normal sequence with some overlap as one bank reaches its full withdrawal position and the next bank begins to withdraw. Interlocks are provided to preclude simultaneous withdrawal of more than two banks of control rods or shutdown rods.

The control system is capable of restoring coolant average temperature to within the programmed temperature deadband, following a scheduled or transient change in load.

The reactor plant can be placed under automatic control in the power range between 15 percent of load and full load and will accept the following design transients while in automatic control:

a) Step load increases of 10% within the load range of 15% to 90% of full power (without turbine bypass)

b) Step load reductions of 10% within the load range of 100% to 25% of full power (without turbine bypass)

c) A 5% per minute ramp load change within the load range – 15% to 100% of full power (without turbine bypass)

d) A -10% to -50% change in load, at a maximum turbine unloading rate of 200% per minute, from approximately 100% load with steam dump (load rejection capability depends on full power Tavg; see Section 7.3.2) (with turbine bypass).

A programmed pressurizer water level as a function of $T_{avg}$ is provided to minimize the requirements of the Chemical and Volume Control and Waste Disposal Systems resulting from coolant density changes during loading and unloading from full power to zero power.

Following a reactor and turbine trip, sensible heat stored in the reactor coolant is removed without actuation of steam generator safety valves by means of controlled steam bypass to the condenser and by injection of feedwater to the steam generators. Reactor Coolant System temperature is reduced to the no load condition. This no load coolant temperature is maintained by steam bypass to the condensers to remove residual heat.

The control system is designed to operate as a stable system over the full range of automatic control throughout core life without requiring operator adjustment of set points other than normal calibration procedures.

7.3.2 <u>System Design</u>

A block diagram of the Reactor Control System is shown in Figure 7.3-1.

Rod Control

There are 53 total RCC assemblies. The assemblies are grouped into (1) 4 shutdown banks having rod clusters of 8, 8, 4, 4, rod clusters and (2), 4 control banks 8, 4, 8 and 9 rod clusters.

Figure 3.2-1 shows the location of the RCC assemblies in the core. The four control banks are the only rods that can be manipulated under automatic control. The banks are divided into groups to obtain smaller incremental reactivity changes. All RCC assemblies in a group are electrically paralleled to step simultaneously. Position indication for each RCC assembly type is the same.

Control Group Rod Control

The Reactor Control System is capable of restoring programmed average temperature following a scheduled or transient change in load. The coolant average temperature is programmed to increase linearly from zero power to the full power conditions.

The control system will also compensate initially for reactivity changes caused by fuel depletion and/or xenon transients. Final compensation for these two effects is periodically made with adjustments of boron concentration. The control system then readjusts the control rods in response to changes in coolant average temperature resulting from changes in boron concentration.

The coolant average temperatures are measured from the hot leg and the cold leg in each reactor coolant loop. The average of the four measured average temperatures is the main control signal. This signal is sent to the control rod programmer through a proportional plus rate compensation unit. The control rod programmer commands the direction and speed of control rod motion. A compensated pressurizer pressure signal, and a power-load mismatch signal are also employed as control signals to improve the plant performance. The power-load mismatch channel takes the difference between nuclear power (average of all four power range channels) and a signal of turbine load (first stage (inlet) turbine pressure), and passes it through a high-pass filter such that only a rapid change in flux or power causes rod motion. The pressure compensation and the power-load mismatch compensation serve to speed up system response and to reduce transient peaks.

The control bank rods are divided into four banks comprising 8, 4, 8 and 9 RCC assemblies respectively, to follow load changes over the full range of power operation. Each control rod bank is driven by a sequencing, variable speed rod drive control unit. The assemblies in each control bank are divided into two groups. The groups are moved sequentially one step at a time. The sequence of motion is reversible, that is, a withdrawal sequence is the reverse of the insertion sequence. The variable speed sequential rod control affords the ability to insert a small amount of reactivity at low speed to accomplish fine control of reactor coolant average temperature about a small temperature deadband. Any reactor trip signal causes the rods to drop by gravity into the core.

Manual control is provided to manually move a control bank in or out at a preselected fixed speed.

Proper sequencing of the RCC assemblies is assured: first, by fixed programming equipment in the Rod Control System, and second, through administrative control of the reactor plant operator. Startup of the plant is accomplished by first manually withdrawing the shutdown rod banks to the full out position. This action requires that the operator select the SHUTDOWN BANK position on a control board mounted selector switch and then position the IN-HOLD-OUT level (which is spring return to the HOLD position) to the OUT position.

RCC assemblies are then withdrawn under manual control of the operator by first selecting the MANUAL position on the control board mounted selector switch and then positioning the IN-HOLD-OUT LEVER to the OUT position. In the MANUAL selector switch position, the rods are withdrawn (or inserted) in a predetermined programmed sequence by the automatic programming equipment.

When the reactor power reaches approximately 15% of rated power, the operator may select the AUTOMATIC position, where the IN-HOLD-OUT lever is taken out of service, and rod motion is controlled by the Reactor Control and Protection Systems. A permissive interlock limits automatic control to reactor power levels above 15%. In the AUTOMATIC position, the rods are again withdrawn (or inserted) in a programmed sequence by the automatic programming equipment.

Programming is set so that as the first bank out (control bank A) reaches a preset position, the second bank out (control bank B) begins to move out simultaneously with first bank. When control bank A reaches the top of the core, it stops, and control bank B continues until it reaches a preset position near the top of the core where control bank C motion beings, etc. The withdrawal sequence continues until the plant reaches the desired power level. The programmed insertion sequence is the opposite of the withdrawal sequence, i.e., the last control bank out is the first control bank in.

With the simplicity of the rod program, the minimal amount of operator selection, and two separate direct position indications available to the operator, there is very little possibility that rearrangement of the control rod sequencing could be made.

Shutdown Rod Control

The shutdown rods together with the control rods are capable of shutting the reactor down. They are used in conjunction with the adjustment of chemical shim to provide shutdown margin of at least one percent following reactor trip with the most reactive control rod in the fully withdrawn position for all normal operating conditions. The shutdown banks are manually controlled during normal operation and are moved at a constant speed with staggered stepping of the groups within the banks. Any reactor trip signal causes them to drop by gravity into the core. They are fully withdrawn during power operation and are withdrawn first during startup. Criticality is always approached with the control rods after withdrawal of the shutdown banks. Four shutdown banks with a total of 24 clusters are provided.

Interlocks

The rod control group is used for automatic control and is interlocked with measurements of turbine-generator load to prevent automatic control rod withdrawal below 15% of nominal power. The manual and automatic controls are further interlocked with measurements of neutron flux, $\epsilon T$ and rod drop indication to prevent approach to an overpower condition.

Rod Drive Performance

The control banks are driven by a sequencing, variable speed rod drive programmer. In each control bank of RCC assemblies, two groups (each containing a small number of RCC assemblies) are moved sequentially in a cycle such that both groups are maintained within one step of each other.

The sequence of motion is reversible, that is, withdrawal sequence is the reverse of the insertion sequence. The sequencing speed is proportional to the control signal from the Reactor Control System. This provides control group speed control proportional to the demand signal from the control system.

The output of two paralleled motor generator (M-G) sets provides power to the rod drive mechanism coils through a solid state control system. Two reactor trip breakers are placed in series with the output of the M-G sets. To permit on-line testing, a bypass breaker is provided across each of the two breakers.

RCCA Position Indication

Two separate systems are provided to sense and display control rod position as described below:

a) Analog System – An analog signal is produced for each individual rod by a linear position transmitter.

   An electrical coil stack is located above the stepping mechanisms of the control rod magnetic jacks, external to the pressure housing, but concentric with the rod travel. When the associated control rod is at the bottom of the core, the magnetic coupling between the primary and secondary coil winding of the detector is small and there is a small voltage induced in the secondary. As the control rod is raised by the magnetic jacks, the relatively high permeability of the lift rod causes an increase in magnetic coupling. Thus, an analog signal proportional to rod position is obtained.

   Direct, continuous readout of every control rod is presented to the operator on individual indicators.

   A deviation monitor alarm is actuated if an individual rod position deviates from its relative bank position by a preselected distance.

   Lights are provided for rod bottom positions for each rod. The lights are operated by bistable devices in the analog system.

b) Digital System – The digital system counts pulses generated in the rod drive control system. One counter is associated with each group of control and shutdown rods. Readouts of the digital system are in the form of electromechanical add-subtract counters reading the number of steps of rod movement with one display for each group. These readouts are mounted on the control panel.

The digital and analog systems are separate systems; each serves as backup for the other. Operating procedures require the reactor operator to compare the digital and analog readings upon recognition of any apparent malfunction. Therefore, a single failure in rod position

indication does not in itself lead the operator to take erroneous action in the operation of the reactor.

Full Length Rod Drive Power Supply

The full length control rod drive power supply concept, using a single trip bus system, has been successfully employed on all Westinghouse PWR Plants. Potential fault conditions with a single trip bus system are discussed in this section. The unique characteristics of the latch type mechanisms with its relatively large power requirements makes this system with the redundant series trip breakers particularly desirable.

The solid state rod control system is operated from two parallel connected 438 kVA generators which provide 260 volt line to line, three phase, four wire power to the rod control circuits through two series connected reactor trip breakers.

This AC power is distributed from the trip breakers to a line-up of identical solid state power cabinets and a DC holding cabinet using a single overhead run of enclosed bus duct which is bolted to and therefore comprises part of the power cabinet arrangement. Alternating current from the motor-generator sets is converted to a pulsed direct current by the power cabinet and is then distributed to the mechanism coils. Each complete rod control system includes a single 125/70 volt DC power supply which is used for holding the mechanisms in position during maintenance of normal power supply.

This 125/70 volt supply, which receives its input from the AC power source downstream of the reactor trip breakers, is distributed to each power cabinet and permits holding mechanisms in groups of four by manually positioning switches located in the power cabinets. The 70/40 ampere output capacity limits the holding capability to eight rods.

Reactor Trip

Current to the mechanisms is interrupted by opening either of the reactor trip breakers. The 125/70 volt DC maintenance supply will also be interrupted since this supply receives its input power through the reactor trip breakers.

Trip Breaker Arrangement

The trip breakers are arranged in the reactor trip switchgear in individual metal enclosed compartments. The 1000 ampere bus work, making up the connections between trip breakers are separated by metal barriers to prevent the possibility that any conducting objects could short circuit, or bypass, trip breaker contacts.

Maintenance Holding Supply

The 125/70 volts DC holding supply and associated switches have been provided to avoid the need for bringing a separate DC power source to the rod control system during maintenance on the power cabinet circuits. This source is adequate for holding a maximum of five mechanisms and satisfies all maintenance holding requirements.

Control System Construction

The rod control system equipment is assembled in enclosed steel cabinets. Three phase power is distributed to the equipment through a steel enclosed bus duct, bolted to the cabinets. DC power connections to the individual mechanisms are routed to the reactor head from the solid state cabinets through insulated cables, enclosed junction boxes, enclosed reactor containment penetrations, and sealed connectors. In view of this type of construction, an accidental connection of either an AC or DC power source, either internal or external to the cabinets, is not considered credible.

AC Power Connections

The three phase four wire supply voltage required to energize the equipment is 260 volts line to line, 58.2 Hz, 438 kVA capacity, zig-zag connected. It is unlikely that any power supply, and in particular one as unusual as this four wire power source could be accidentally connected, in phase, in the required configuration. Also it should be noted that this requires multiple connections, not single connections. The closest outside sources available in the plants are 480 volt auxiliary power source and 208 volt lighting source.

Connections of either a 480 or 208 volt, 60 Hz source to the single AC bus supplying the rod control system causes currents to flow between the sources due to an out of phase condition. These currents flow until the generator accelerates to a speed synchronous with the 60 Hz outside source, a time sufficient to trip the generator breakers. The out-of-phase currents for an unlimited capacity outside source, an outside source with a capacity equivalent to the normal generator kVA, and for either one or two M-G sets in service are tabulated below:

Out of Phase Currents (Amperes)

| | One M-G Set in Service | Two M-G Sets In Service |
|---|---|---|
| 480 volts | | |
| Unlimited Capacity | 25,000 | 50,000 |
| 438 kVA Capacity | 12,000 | 25,000 |
| 208 volts | | |
| Unlimited Capacity | 16,000 | 32,000 |
| 438 kVA Capacity | 8,000 | 16,000 |

All of the foregoing currents are sufficiently high to trip out the generator breakers on either overcurrent or reverse current. This trip-out is detectable by annunciation in the Control Room. If the outside power source trips, the connection is of no concern.

Each solid state power cabinet is tied to the main AC bus through three fused disconnect switches; one for the stationary gripper coil circuits, one for the movable gripper coil circuits, and one for the lift coil circuits. Reference voltage to operate the control circuits for all three coil circuits must be in phase with the supply to all coil circuits for proper operation of the system. If the outside power source were brought into an individual cabinet, nine (9) normal source connections would have to be disconnected and the outside source would have to be tied in phase to the proper nine (9) points plus one (1) neutral point to allow movement of the rods. This is not considered credible.

Connection of a single phase AC source (i.e., one line to neutral) is also considered improbable. This would again require a high capacity source which would have to be connected in-phase with the non-synchronous M-G set supply. Again, more than one connection is needed to achieve this condition. Each power cabinet contains three alarm circuits (stationary, movable and lift) that would annunciate the condition to the operator. In addition, calculations show that a single phase source of 208 volts, 260 volts, or 480 volts will not supply enough current to hold the rods. Therefore, a jumper across two trip circuit breaker contacts in series which results in a single phase remaining closed would not provide sufficient current to hold up the rods.

The normal source generators are connected in a zig-zag winding configuration to eliminate the effects of direct current saturation of the machines resulting from the direct currents that flow in the half wave bridge rectifier circuits. If this connection were not used, the generator core would saturate and loss of generating action would occur. This condition would also occur in a transformer. An outside source not having the zig-zag configuration would have to have a large capacity (400 kVA) to avoid the loss of transformer action from saturation.

Most of the components in the equipment are applied with a 100% safety factor. Therefore, the possibility exists that the system will operate at 480 volts with a source of sufficient capacity. The system will definitely operate at 208 volts with a source of sufficient capacity.

The connection of an outside source of AC power to one rod control system would first require a need for this source. No such need exists since two power sources (M-G sets) are already provided to supply the system. If the source were connected in spite of the need, extreme measures would have to be taken by the intruder to complete the connection. The outside source would have to be a large capacity (400 kVA) one. The currents that flow would require the routing of large conductors or bus bars, not the usual clip leads. Then the disassembly of switchgear or enclosed bus duct would be required to expose the single AC bus. Large bolted cable or bus bar terminations would have to be completed. A total of four conductors would have to be connected in phase with a non-synchronous source. To expect that a connection could be completed with the equipment either energized or de-energized in view of the obstacles which would prevent such a connection is incredible.

However, even if the connection were completed, the outside source connection would be detectable by the operator through the tripping of the generator breakers.

DC Power Connections

An external DC source could, if connected inside the power cabinet, hold the rods in position. This would require a minimum supply voltage of 50 volts. Since the holding current for each mechanism coil is 4 amperes, the DC current capacity would have to be approximately 180 amperes to hold all rods. Achieving this situation would require several acts – bringing in a power source which is not required for any type of operation in the rod control system, preferentially connecting it into the system at the correct points, and actuating specific holding switches so as to interconnect all rods. Closure of twelve switches in four separate cabinets would be required to hold all rods. One switch could hold as many as four rods.

The application of a DC voltage to an individual rod external to the power cabinet would affect only a single rod connection with other rods in the group being prevented by the blocking diodes in the power circuits.

Should an external DC source be connected to the system, the system is provided with features to permit its detection.

Each solid state power cabinet contains circuitry which compares the actual currents in the stationary and movable gripper coils with the reference signals from the step sequencing unit (slave cycler). In taking a single step, the current to the stationary gripper coil will be profiled from the holding value to the maximum, to zero and return to holding level. Correspondingly, the movable gripper coil must change from zero to maximum and return to zero. The presence of an external DC source on either the stationary or movable would prevent the related currents from returning to zero.

This situation would be instantaneously annunciated by way of the comparison circuit. Therefore, any rod motion would actuate an alarm indicating the presence of an external DC source. In addition, an external DC source would prevent rods from stepping. Thus, an external source could be detected by the rod position indication system indicating failure of the rod(s) to move.

Connection of an external DC power source to the output lines of the 125/70 volt DC power supply can be detected by opening the three phase primary input of the supply and checking the output indication lights.

Evaluation Summary

In view of the preceding discussion, the postulated connection of an external power source (either AC or DC) or occurrence of short circuits that could prevent dropping of the rods is not considered credible.

Specifically:

a) The need for an outside power source has been eliminated by incorporating built-in holding sources as part of the rod control system and by providing two M-G sets.

b) The equipment is contained within enclosed steel cabinets precluding the possibility of an accidental connection of either AC or DC power in the cabinets.

c) AC power distribution is accomplished using steel enclosed bus duct. The high capacity (438 kVA) AC power source is unique and not readily available. Multiple connections are required.

d) DC power is distributed to the individual mechanisms through insulated cables and enclosed electrical connections precluding the accidental connection of an outside DC source external to the cabinets. The high capacity DC source required to hold rods is not readily available in the rod control system, would require multiple connections, and would require deliberate positioning of switches within the enclosed cabinets.

e) Provisions are made in the system to permit detection of an external DC source which could preclude a rod release.

The total capacity of the system including the overload capability of each motor generator set is such that single set out of service does not cause limitations in rod motion during normal plant

operation. In order to minimize reactor trip as a result of a unit malfunction, the power system is normally operated with both units in service.

Turbine Bypass

A turbine bypass system is provided to accommodate a reactor trip with turbine trip and in conjunction with automatic reactor control can accommodate a load rejection without reactor and turbine trip. The maximum load rejection that can be accommodated without reactor and turbine trip depends on the full load Tavg. A maximum of a 10% load rejection can be accommodated for the minimum acceptable full load Tavg of 550.6°F. As the full load Tavg is increased, larger load rejections can be accommodated. For full load Tavg values of 565 °F or higher, load rejections of 50% can be accommodated. The turbine bypass system removes steam to reduce the transient imposed upon the reactor coolant system so that the control rods can reduce the reactor power to a new equilibrium value without allowing overtemperature, overpressure conditions in the Reactor Coolant System.

The steam dump is actuated by an electrical load decrease rate greater than a preset value. This signal supplies air to the dump valves, which then allows them to open and close according to the temperature error signal, a compensated ($T_{avg} - T_{ref}$) signal. The dump valves modulate open proportionally to this temperature error signal with a stroke time of approximately 20 seconds. For large temperature errors the valves will trip open in two banks as required for fast response with a stroke time of about three seconds. Upon reduction of the error signal below the trip-open setpoints, the respective valve groups return to modulating control.

The steam dump decreases proportionally as the control rods act to reduce the coolant average temperature. The artificial load is therefore removed as the coolant average temperature is restored to its programmed value. When steam dump is no longer required, the air supply to the valves may be manually removed.

Since the steam dump valves exhaust into the condenser, all steam dump is blocked when the condenser in unavailable.

The turbine bypass steam system is described in Section 10.2. The bypass flows to the main condenser.

Feedwater Control

Each steam generator is equipped with two three element feedwater control systems (one for the main regulator valve and the second for the low flow regulator valve) which maintain a programmed water level as a function of load on the secondary side of steam generator. The three element feedwater control system continuously compares actual feedwater flow with steam flow compensated by steam pressure with a water level set point to regulate the feedwater valve opening. The individual steam generators are operated in parallel, both on the feedwater and on the steam side.

Continued delivery of feedwater to the steam generator is required as a sink for the heat stored and generated in the coolant following a reactor trip and turbine trip. A reactor trip signal provides an override signal to the feedwater control system. After a trip, all feedwater valves open fully thereby insuring the full supply of feedwater following a reactor trip and turbine trip. Another override signal then closes the feedwater valves when the coolant average temperature

falls below a preset temperature value or when the respective steam generator level rises to a preset value. Manual override of the feedwater control systems is also provided.

Pressure Control

The reactor coolant system pressure is maintained at constant value by using heaters in the water region and spray in the steam region of the pressurizer. Electrical immersion heaters are located near the bottom of the pressurizer. A portion of the heater groups are proportional heaters and are used for small pressure variation control and to compensate for heat losses and the smaller continuous spray. Up to three sets of backup heaters may be turned on manually and operated continuously. The remaining (backup) heaters are turned on either when the pressurizer pressure controller signal is below a preset value or when the pressurizer level exceeds the programmed level setpoint by a preset amount.

The spray valves for the pressurizer are located near their respective RCS cold legs, and the spray nozzle is located at the top of the pressurizer. Spray is initiated when the pressure controller signal is above a preset set point. Spray rate increases proportionally with increasing pressure until it reaches the maximum spray capacity.

Steam condensed by spray reduces the pressurizer pressure. A small continuous spray is normally maintained to reduce thermal stress and thermal shock when the spray valves open and help maintain uniform water chemistry and temperature in the pressurizer.

Two power operated relief valves (PORVs), PCV-455C and PCV-456, prevent the RCS pressure from exceeding the Technical Specifications limits of 10 CFR 50 Appendix "G" during low temperature, low pressure and water solid modes of operation. The PORVs are armed below a preset temperature of 319°F, and will open at a programmed pressure which is set to prevent exceeding the Appendix "G" curves. The two PORVs are supplied with nitrogen. The instrument $N_2$ system for the PORVs is tapped from the $N_2$ supply line to the four safeguards accumulators. The accumulators are sized to provide for 200 valve operating cycles. The actual take-off point for this $N_2$ system is downstream of the pressure regulator valve NNE-863. The PORV accumulators individually hold 6 cu ft of $N_2$ at a minimum pressure of 550 psig. During low temperature shutdown operations, the Overpressure Protection System requires an $N_2$ supply of sufficient capacity which, in case of loss of main $N_2$ supply, can support the number of PORV cycles resulting from an overpressure event of 10 minute duration. This $N_2$ supply is provided by one Safety Injection Accumulator having its associated $N_2$ fill valve blocked open.

One PORV is operated on the pressurizer pressure controller signal, the other one is operated on the actual pressure signal. A separate interlock is provided for each so that if a second pressure channel indicates abnormally low, are the time the relief valve operation is called for by the other channel, the valve activation is blocked. The logic for each is thus basically two out of two. However, during normal operation at normal pressure, the interlock is not actuated and only the operating signals are required to actuate the valve. The interlock is set above normal operating pressure to prevent spurious operation.

Three spring-loaded safety valves limit system pressure to 2750 psia following a complete loss of load without direct reactor trip or actuation of turbine bypass.

Reactor coolant flow to the residual heat removal loop is from the hot leg of Loop 2 through two motor operated valves (No. 731 and 730). Valves 731 and 730 are pressure interlocked to prevent opening should reactor coolant pressure go above 450 psig. This arrangement

prevents inadvertent pressurization of the residual heat removal loop when the Reactor Coolant System is above 450 psig. These valves will be opened when RCS pressure is lower than 450 psig. Valve position indication lights and position selector switches for both valves are provided in the control room. These valves are closed during power operation to preclude RHRS over-pressurization. To open the valve, the switch is held over to the Open position and if RCS pressure is less than 450 psig, the valve will open. If these valves are open and RCS pressure increases to 550 psig, they will auto-close. A narrow range pressure recorder with an operator controlled alarm point, which actuates warning lights and audible device, has been added to instrument loop for PT-402. This is designed to attract the operators attention to a potential overpressure transient in progress, to allow him to take necessary action to minimize the magnitude of overpressure event while the RCS is operating at low pressure. The system is not required for safe shutdown of the reactor, and the operator may deactivate the recorder and alarms, which removes the potential for distracting alarms when a normal RCS pressure.

To prevent inadvertent isolation of the RHR loop when the Reactor Coolant System is below 200 degrees, depressurized, and vented to an equivalent opening of greater than two (2) square inches AC-MOV-730 and 731 may be de-energized open.

These valves are also interlocked with containment sump valves 885A and B. To open valves 885A and B, the RHR suction valves 730 and 731, respectively, must be closed. This prevents the reactor coolant water from being drained to the contained sump. High Head SI Suction Valves 888A and B are also interlocked with valves 730 and 731, respectively. A valve 884A and B will not open if 730 and 731, respectively, are opened.

SI-MOV-883 is interlocked with AC-MOV-730 and AC-MOV-731 so that the valve can only be opened if both MOV-730 and MOV-731 are fully closed. If valve SI-MOV-883 is open and valve AC-MOV-730 or AC-MOV-731 leave their closed limit seats, valve SI-MOV-883 will auto-close. The interlock prevents inadvertent opening of valve SI-MOV-883 during cool down and subsequent diversion of reactor coolant to the RWST or over pressurization of a lower pressure SI piping system.

Valves AC-MOV-730 and -731 may be de-energized during cold shutdown if the RCS is depressurized and vented through a minimum equivalent opening of two (2) square inches. De-energizing these valves while the RHR pumps are in service prevents inadvertent isolation of the RHR pump suction supply, which could potentially cause pump failure. De-energizing these valves will also cause a loss of all of the interlock protection associated with AC-MOV-730 and -731. When AC-MOV-730 and –731 are de-energized, administrative controls are established to replace the protective functions of these interlocks. These administrative controls prevent unanticipated communication of reactor coolant with the containment sump and the RWST. These controls also prevent overpressurization of the RHR and SI system piping and components.

### 7.3.3 System Design Evaluation

#### Plant Stability

The control system is designed to maintain a stable reactor coolant average temperature within acceptable limits. Continuous oscillation at a low frequency and small amplitude is expected. Proper adjustment of the control loop static and dynamic gains (with respect to the process response) can reduce this oscillation almost to zero and will also avoid instability induced by the control system itself. Because stability is more difficult to maintain at low power under

automatic control, no provision is made to provide automatic control below 15 percent of full power.

The control system is designed to operate as a stable system over the full range of automatic control throughout core life.

Step Load Changes Without Turbine Bypass

A typical reactor power automatic control requirement is to restore equilibrium conditions without a plant trip, following 10 percent step load demand increases within the range of 15 to 90 percent of full power and 10% step load demand reductions within the range of 100% to 25% of full power. The design was necessarily based on conservative conditions and a greater transient capability is expected for actual operating conditions. A load demand greater than full power is inhibited by the turbine control load limit devices in response to input from the Reactor Protection System. Although turbine bypass is provided for added control after large load decreases, it will not be necessary during the 10% load changes.

The function of the control system is to minimize the reactor coolant average temperature deviation during the transient within an acceptable value and to restore average temperature to the programmed set point within an acceptable time. Excessive pressurizer pressure variations are prevented by using spray and heaters in the pressurizer.
The margin to over-temperature $\Delta T$ reactor trip is of primary concern for the step load changes. This margin is influenced by nuclear flux, pressurizer pressure, and reactor coolant average temperature and temperature rise across the core.

Ramp Loading and Unloading

Ramp loading and unloading is provided over the 15 to 100 percent power range under automatic control. The function of the control system is to maintain the coolant average temperature and the secondary steam pressure as functions of turbine-generator load within acceptable deviation from the programmed values. The minimum control rod speed provides a sufficient reactivity rate to compensate the reactivity changes resulting from the moderator temperature coefficient and the power coefficient.

The coolant average temperature is increasing during loading and there is a continuous in-surge to the pressurizer resulting from coolant expansion. The sprays limit the resulting pressure increase. Conversely, as the coolant average temperature is decreasing during unloading, there is a continuous out-surge from the pressurizer resulting from coolant contraction. The heaters limit the resulting system pressure decrease. The pressurizer level is programmed such that the water level has an acceptable margin above the low level heater cutout set point during the loading and unloading transients.

The primary concern for the loading is to limit the overshoot in coolant average temperature to provide sufficient margin to the over-temperature $\Delta T$ trip.

The automatic load controls are designed to safely adjust the unit generation to match load requirements within the limits of the unit capability and licensed rating.

Loss of Load With Turbine Bypass

The Reactor Control System is designed to accept a 10% to 50% (depending on full power Tavg; see Section 7.3.2) loss of load accomplished as a turbine runback at a maximum rate of 200% per minute without requiring a reactor trip. The automatic turbine bypass system is able to accommodate this abnormal load rejection by reducing the thermal transient imposed upon the reactor coolant system. The reactor power is reduced at a rate consistent with the capability of the rod control system. The reducing of the reactor power is automatic down to 15 percent of full power. Manual control is used when the power is below this value. The steam bypass is removed as fast as the control rods are capable of inserting negative reactivity.

The pressurizer relief valves might be actuated for the most adverse conditions, e.g., the most negative Doppler coefficient, and the minimum incremental rod worth. The relief capacity of the power operated relief valves is sized large enough limit the system pressure to prevent actuation of high pressure reactor trip for the most adverse conditions.

Turbine-Generator Trip With Reactor Trip

Turbine-generator unit trip is accompanied by reactor trip. With a secondary system design pressure of 1100 psia, the plant is operated with a programmed average temperature as a function of load, with the full load average temperature significantly greater than the saturation temperature corresponding to the steam generator safety valve set point. This, together with the fact that the thermal capacity in the Reactor Coolant System is greater than that of the secondary system, requires a heat sink to remove heat stored in the reactor coolant to prevent actuation of steam generator safety valves for turbine and reactor trip from full power.

This heat sink is provided by the combination of controlled release of steam to the condenser and by makeup of cold feedwater to the steam generators. The turbine bypass system is controlled from the reactor coolant average temperature signal whose reference set point is reset upon trip to the no load value. Turbine bypass actuation must be rapid to prevent steam generator safety valve actuation. With the bypass valves open the coolant average temperature starts to reduce quickly to the no load set point. The automatic control of reactor coolant average temperature acts to proportionally close the valves and thus minimize the total amount of steam bypassed.

Following turbine trip, the steam voids in the steam generators will collapse and the fully opened feedwater valves will provide sufficient feedwater flow to restore water level in the downcomer. The feedwater flow is cut off if the reactor coolant average temperature decreases below a preset temperature value or if the steam generator water level reaches a preset high set point.

Additional feedwater makeup may then be controlled manually to restore and maintain steam generator level while maintaining the reactor coolant at the no load temperature. Long term residual heat removal is maintained by the steam generator pressure controller (manually selected) which controls the steam pressure (and thus, indirectly, the temperature) by adjusting the amount of turbine bypass to the condensers. The controller operates the same bypass valves to the condensers which are controlled by coolant average temperature during the initial transient following turbine and reactor trip.

The pressurizer pressure and water level fall very fast during the transient resulting from the coolant contraction. If heaters become uncovered following the trip, the Chemical and Volume Control System will provide full charging flow to restore water level in the pressurizer. Heaters are then turned on to heat up pressurizer water and restore pressurizer pressure to normal.

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

## 7.4 EXCORE NUCLEAR INSTRUMENTATION

### 7.4.1 Design Bases

The General Design Criteria presented and discussed in this section are those which were in effect at the time when Indian Point 3 was designed and constructed. These general design criteria, which formed the basis for the Indian Point 3 design, were published by the Atomic Energy Commission in the Federal Register of July 11, 1967, and subsequently made a part of 10 CFR 50.

The Authority has completed a study of compliance with 10 CFR Parts 20 and 50 in accordance with some of the provisions of the Commission's Confirmatory Order of February 11, 1980. The detailed results of the evaluation of compliance of Indian Point 3 with the General Design Criteria presently established by the Nuclear Regulatory Commission (NRC) in 10 CFR 50 Appendix A, were submitted to NRC on August 11, 1980, and approved by the Commission on January 19, 1982. These results are presented in Section 1.3.

Fission Process Monitors and Controls

Criterion: Means shall be provided for monitoring or otherwise measuring and maintaining control over the fission process throughout core life under all conditions that can reasonably be anticipated to cause variations in reactivity of the core. (GDC 13 of 7/11/67)

The excore Nuclear Instrumentation System is provided to monitor reactor power from source range, through intermediate range and power range, up to 120 percent of full power. The system provides indication, control and alarm signals for reactor operation and protection.

Additionally, per Regulatory Guide 1.97 requirements, an Excore Neutron Flux Monitoring System (NFMS) (see Plant Drawing 9321-LL-96553 [Formerly Figure 7.4-4]) consisting of two detectors has been installed to provide reactor power indication from source range through power range. The Regulatory Guide 1.97 excore Neutron Flux Monitoring System provides local indication elsewhere in the plant, in addition to indication only provided to the control room via QSPDS and CFMS. These other indication locations are in the upper electrical tunnel and at the charging station in the PAB for use during shutdown from outside the control room.

The operational status of the reactor is monitored from the Control Room. When the reactor is subcritical (i.e., during cold or hot shutdown, refueling and approach to criticality) the relative reactivity status (neutron source multiplication) is continuously monitored and indicated by proportional counter detectors located in instrument wells in the primary shield adjacent to the reactor vessel. Two source range detector channels are provided for supplying information on multiplication while the reactor is subcritical. A reactor trip is actuated from either channel if the neutron flux level becomes excessive. This system is checked prior to operations in which criticality may be approached. This is accomplished by the use of an incore source to provide a meaningful count rate even at the refueling shutdown condition. Any appreciable increase in the neutron source multiplication is slow enough to give ample time to start corrective action (boron dilution stop and/or emergency boron injection) to prevent the core from becoming critical

When the reactor is critical, means for showing the relative reactivity status of the reactor are:

1) Rod Position

2) Source, Intermediate and Power Range Detector Signals

3) Qualified Safety Parameters Display System (QSPDS)

4) Boron Concentration

5) Hot Leg Temperatures

The position of the control banks is directly related to the reactivity status of the reactor when at power, and any unexpected change in the position of the control banks under automatic control or change in the hot leg coolant temperature under either manual or automatic control provides a direct and immediate indication of a change in the reactivity status of the reactor. Periodic samples of the coolant boron concentration are taken. The variation in concentration during core life provides a further check on the reactivity status of the reactor including core depletion.

High nuclear flux protection is provided both in the power and intermediate ranges by reactor trips, actuated from either range, if the neutron flux level exceeds trip set-points. When the reactor is critical, the best indication of the reactivity status in the core (in relation to the power level and average coolant temperature) are the control room display of the rod control group position and the boron concentration in the coolant.

7.4.2 System Design

Nuclear Instrumentation System (NIS)

The three instrumentation ranges of the Nuclear Instrumentation System (NIS) overlap so that continuous readings are available during transition from one range to another. The sensitivities of the neutron detectors are illustrated on Figure 7.4-1. The Nuclear Instrumentation System diagram is shown on Figure 7.4-2.

Detectors

The excore system consists of twelve independent detectors in six instrument wells located around the reactor, as shown in Figure 7.4-3. The six assemblies provide the following instrumentation:

1. Power Range

   This range consists of four independent, long, uncompensated ionization chamber assemblies. Each assembly is made up of two sensitive lengths. One sensitive length covers the upper half of the core, and the other length covers the lower half of the core.

   In effect the arrangement provides a total of eight separate ionization chambers approximately one-half the core height. The eight uncompensated (guard-ring) ionization chambers sense thermal neutrons in the range from $5.0 \times 10^{2}$ to $1.0 \times 10^{11}$ neutrons per sq cm per sec.

   Each chamber initially had a nominal sensitivity of $3.1 \times 10^{-13}$ amperes per neutron per sq cm (see Figure 7.4-1). The four long ionization chamber assemblies are located in vertical instrument wells adjacent to the four "corners" of the core. The

assembly is manually positioned in the assembly holders and is electrically isolated from the holder by means of insulated standoff rings.

Due to redesign of the Nuclear Core (low leakage core design) and resultant decrease in thermal neutrons at the detectors, new Power Range Moderators have been installed on the four (4) Power Range uncompensated ionization chambers. The Power Range Moderators increase the normal sensitivity of the chambers by approximately 700%.

2. Startup Range (Intermediate and Source)

There are two separate startup range assemblies. Each assembly contains one compensated ionization detector (intermediate range) and one proportional counter detector (source range).

The source range neutron detectors are proportional counters with an initial nominal sensitivity of 10 counts per sec per neutron per sq cm per sec (see Figure 7.4-1). The detectors sense thermal neutrons in the range from $10^{-1}$ to 5. x $10^{5}$ neutrons counts per second. The range of the source range channel is $10^{0}$ to $10^{6}$ counts per second.

The Source Range detectors are positioned in detector assembly containers by means of a linear, high density moderator insulator. The detector and insulator units are packaged in a housing which is inserted into the detector wells. The detector assembly is electrically isolated from the detector well by means of insulated stand-off rings.

The intermediate range neutron detectors are compensated ionization chambers that sense thermal neutrons in the range form 2.5 x $10^{2}$ to 2.5 x $10^{10}$ neutrons per sq cm per sec and initially had a nominal sensitivity of 4 x $10^{-14}$ amperes per neutron per sq cm per second (see Figure 7.4-1). They produce a corresponding direct current of $10^{-11}$ to $10^{-3}$ amp. These detectors are located in the same detector assemblies as the proportional counters for the source range channels.

Other than the source range pre-amplifier, which is located in containment, the electronic components for each of the source, intermediate and power range channels for the NIS are contained in a draw-out- panel mounted in racks in the Control Room.

Power Range Channel

There are three sets of power range measurements. Each set utilizes four individual currents as follows:

a) Four currents directly from the lower sections of the long ionization chambers

b) Four currents directly from the upper sections

c) Four total currents of (a) and of (b), equivalent to the average of each section.

For each of the four currents in (a) and (b), the current measurement is indicated directly by a microammeter, and isolated signals are available for control console indication and recording. An analog signal proportional to individual currents is transmitted through buffer amplifiers to the

overtemperature ΔT channel and provides automatic reset of the trip point for these protection functions. The total current, equivalent to the average, is then applied through a linear amplifier to the bistable trip circuits. The amplifiers are equipped with gain and bias controls for adjustment to the actual output corresponding to 100 percent of rated reactor power.

Each of the four amplifiers also provides amplified isolated signals to the main control board for indication and for use in the Reactor Control System. Each set of bistable trip outputs is operated as a two-out-of-four coincidence to initiate a reactor trip. Bistable trip outputs are provided at low and high power set points depending on the operating power. To provide more protection during startup operation the low range power bistable is used. This trip is manually blocked after a permissive condition is obtained by two of four power range channels. The high power trip bistable is always active.

The overpower trip is set so that, with the maximum instrumentation and bistable set point error, the maximum reactor overpower condition will be limited to 118 percent. This limit is accomplished by the use of solid state instrumentation and long ionization chambers, which permit an integration of the flux external to the core over the total length of the core, thereby reducing the influence of axial flux distribution changes due to control rod motion.

The ion chamber current of each detector is measured by sensitive meters with an accuracy of 0.5 percent. A shunt assembly and switch in parallel with each meter allow selection of one of four meter ranges. The available ranges are 0-100, 0-500, 0-1,000 and 0-5,000 microamperes. The shunt assemblies are designed in such a manner that they will not disconnect the detector current to the summing assembly upon meter failure or during switching. An isolation amplifier provides an analog signal proportional to ion chamber current for recording, data logging and delta flux indication. A test calibration unit provides necessary swtiches and signals for checking and calibrating the power range channels.

The linear amplifier accepts the output currents from each of the two chamber sections and derives a nuclear power signal proportional to the summed direct currents. This unit amplifies the currents and converts the normal current signal to a voltage signal suitable for operation of associated components such as bistables and isolation amplifiers.

Multiple power supplies furnish necessary positive and negative voltages for the individual channels and detector power.

Mounted on the front panel of each power range channel drawer are the ion chamber current meters, the shunt selector switches with appropriate positions, and the nuclear power indicator (0 to 120 percent of full power).

The isolated nuclear power signals are available for recording by the nuclear instrumentation system recorder. An isolated nuclear power signal is available for recording overpower conditions up to 200% of full power.

Alarm signals for dropped-rod-rod stop, overpower-rod stop, overpower (low and high range)-reactor trips, and channel tests are annunciated on the main control board. Control signals which are sent to the reactor control and protection system include dropped-rod-rod stop, overpower-rod stop, overpower-reactor trip, and permissive circuit signals. These are described in Section 7.2

Over-riding the turbine runback and rod stop signals from a Power Range Nuclear Instrument Dropped Rod circuit in a single channel, or over-riding any turbine runback signal alone has no impact on reactor safety.

Intermediate Range Channels

There are two intermediate range channels which utilize two compensated ionization chambers. Direct current from the ion chambers is transmitted through triaxial cables to transistor logarithmic current amplifiers in the nuclear instrumentation equipment.

The logarithmic amplifier derives a signal proportional to the logarithm of the current as received from the output of the compensated ion chamber. The output of the logarithmic amplifier provides an input to the level bistables for reactor protection purposes and source range cutoff. The bistable trip units are similar to those in the other ranges. The trip outputs can be manually blocked after receiving a permissive signal from the power range channels. On decreasing power, the intermediate range trips for reactor protection are automatically inserted when the power range permissive signal is not present.

Low voltage power supplies contained in each drawer furnish the necessary positive and negative voltages for the channel electronic equipment. Two medium voltage power supplies, one in each channel, furnish compensating voltage to the two compensated ion chambers. The high voltage for the compensated ion chambers is supplied by separate power supplies also located in the intermediate range drawers.

Neutron (log N) flux level indicators are mounted, one each, on the front panel of the intermediate range channel cabinet and on the control board. These indicators are calibrated in terms of ion chamber current ($10^{-11}$ to $10^{-3}$ amp).

Isolated neutron flux level signals are available for recording and startup rate computation. The startup rate for each channel is indicated at the main control board in terms of decades per minute over the range of –0.5 to 5.0 DPM.

Channel test, high flux level rod stop, and reactor trip signals are alarmed on the main control board annunciator. The latter signal is sent to the Reactor Protection System.

Source Range Channels

There are two source range channels utilizing proportional counter detectors. Neutron flux, as measured in the primary shield area, produces current pluses in the detectors. These preamplified pulses are applied to transistor amplifiers and discriminators located in the racks. Triaxial cable is used for all interconnections from the detector assemblies to the instrumentation in the racks. The preamplifiers are located inside the Reactor Containment.

These channels indicate the source range neutron flux and startup rate. They provide high flux level reactor trip and alarm signals to the Reactor Control and Protection Systems. The reactor trip signal is manually blocked when a permissive signal from the intermediate range is available. These channels are also used at shutdown to provide audible alarms in the Reactor Containment and Control Room of any inadvertent increase in reactivity. An audible count rate signal is used during initial phases of startup and is audible in both the Reactor Containment and Control Room.

Amplifiers are used to obtain a high level signal prior to elimination of noise and gamma pulses by the discriminator. The discriminator output is shaped for use by the log integrator.

The log integrator generates an analog signal proportional to the logarithm of the number of pulses per unit time as received from the output of the previous unit. This unit performs log integration of the pulse rate to determine the count rate, and a linear amplifier amplifies the log integrator output for indication, recording, control, and rate computation through isolation amplifiers.

Each source range channel contains two bistable trip units. Both units trip on high flux level, but one is used during shutdown to alarm reactivity changes and the other provides overpower protection during shutdown and startup. The shutdown alarm unit is blocked manually prior to startup or can serve as a startup alarm. When the input to either unit below its set point, the bistable is in its normal position and assumes a "fully-on" status. When an input from the log amplifier reaches or exceeds the set point, the unit reverses its condition and goes "fully-off." The output of the reactor trip unit controls relays in the Reactor Protection System.

Power supplies furnish the protective and negative voltages for the transistor circuits, the alarm lights, and the adjustable high voltage for the neutron detector.

A test calibration unit can insert selected test or calibration signals into the preamplifier channel input or the log amplifier input. A set of precalibrated level signals are provided to perform channel tests and calibrations. An alarm is registered on the main control board annunciator whenever a channel is being tested or calibrated. A trip bypass switch is also provided to prevent a reactor trip during channel test under certain reactor conditions.

The neutron detector high-voltage cutoff assembly receives a trip signal when a one-out-of-two matrix, controlled by intermediate range channel flux level bistables, and manual block condition are present. The cutoff assembly disconnects the voltage from the source range channel high voltage power supply to prevent operation of the proportional counter outside its design range. High voltage and reactor trip circuits are reactivated automatically when two of the intermediate range signals are below the permissive trip setting.

Mounted on the front panel of the source range channel is a neutron flux level indicator calibrated in terms of count rate level ($10^0$ to $10^6$ cps). Mounted on the control board is a neutron count rate level indicator (100 to 106 cps). Isolated neutron flux signals are available for recording by the Nuclear Instrumentation System recorder and for startup rate computation. The startup rate for each channel is indicted at the main control board in terms of decades per minute over the range of –0.5 to +5.0 DPM. The isolation network for these signals prevents any electrical malfuncton in the external circuitry from affecting the signal being supplied to the flux level bistables. The signals for the channel test, high neutron flux at shutdown, and source range reactor trip are alarmed on the main control board annunciator.

Excore Neutron Flux Monitoring System

The Excore Neutron Flux Monitoring System consists of two redundant trains, each with a Wide range flux detector, locally mounted amplifier and processor, local indications and dedicated penetration feedthroughs and cabling (see Plant Drawing 9321-LL-96553 [Formerly Figure 7.4-4]). Detector sensitivities are illustrated on Figure 7.4-1).

Each of the detectors are fission chambers consisting of two aluminum electrodes electroplated with uranium, insulators and fill gas all included in a titanium assembly. The detectors are located at the 90' and 270' instrument wells and replace the back-up source range detectors that were originally located there. (See Figure 7.4-3)

The amplifiers and microprocessors are located outside the Containment Building in the electrical penetration area in local panels. Redundant trains are powered by redundant instrument bus power supplies. Through isolation devices the Excore Neutron Flux Monitoring System provides the 10 CFR 50, Appendix R, and Reg. Guide 1.97 required shutdown signal. Although both channels provide local and control room (via QSPDS & CFMS) indication, only the detector at the 270' location has the alternate electrical feed capability for Appendix R.

The magnitude of the neutron flux in the reactor core is proportional to the fission power in the reactor. The number of neutron pulses per unit time from the detector is proportional to the magnitude of the neutron flux at the detector and since this magnitude is proportional to the neutron flux in the core, the detector pulse rate is therefore proportional to reactor power.

The number of pulses from the detector is monitored and the mean square value of the variance signal from the detector is measured. This mean square value is proportional to the average rate of neutron pulses. The signal processor takes this signal and processes it into a measure of the logarithm of the countrate, the rate of change of countrate, the logarithm of reactor power and the rate of change of reactor power. It provides analog voltage outputs for each of these signals and also provides the isolated outputs as required.

Auxiliary Equipment

Comparator Channel

The comparator channel compares the four nuclear power signals of the power range channels with one another. A local alarm on the channel is actuated when any two channels deviate from one another by a preset adjustable amount. During full power operation, the comparator serves to sense and annunciate channel failures and/or deviations.

Dropped rod Protection

As backup to the primary protection for the dropped RCC accident, i.e., the rod bottom signal, independent detection is provided by means of the out-of-core power range nuclear channels. The dropped-rod sensing unit contains a difference amplifier, which compares the instantaneous nuclear power signal with an adjustable power lag signal and responds with a trip signal to the bistable amplifier when the difference exceeds a preset adjustable amount. Above a given power level, the signal blocks automatic rod withdrawal and initiates protective action in the form of a turbine load cutback. No credit is taken in the dropped rod accident analysis for turbine runback.

Audio Count Rate Channel

The auto count rate channel provides audible source range information during refueling operations in both the Control Room and the Reactor Containment. In addition, this channel signal is fed to a scaler-timer assembly which produces a visual display of the count rate for an adjustable sampling period.

Recorders

One large, two-pen strip chart recorder is mounted on the main control board for recording the complete range of the source and intermediate channels. It is also possible to record any two power range channels as linear signals. Variable chart speeds have been provided.

Switching of inputs to the recorders does not cause any spurious signals that would initiate false alarms or reactor trips.

Two two-pen recorders are provided to record the flux level from each of the four nuclear power range quadrants.

Power Supply

The Nuclear Instrumentation System is powered by four 120 volts AC independent vital bus circuits. (See Chapter 8)

7.4.3 System Evaluation

Loss of Power

The nuclear instrumentation draws its primary power from vital instrument buses discussed in Chapter 8.

Loss of nuclear instrumentation power would result in the initiation of all reactor trips associated with the channel power failure. In addition, all trips which were blocked prior to loss would be unblocked and initiated.

Reliability and Redundancy

The requirements established for the reactor protective system apply to the nuclear instrumentation. All channel functions are independent of every other channel.

Safety Factor

The relations of the power range channels to the Reactor Protective System has been described in Section 7.2. To maintain the desired accuracy in trip action, the total error from drift in the power range channels is held to ±1 percent of full power. Routine tests and recalibration ensure that this degree of deviation is not exceeded. Bistable trip set points of the power range channels are also held to an accuracy of ±1 percent of full power. The accuracy and stability of the equipment were verified by vendor tests.

Overpower Trip Set Point

The overpower trip set point for the Indian Point 3 Reactor is 109%. This trip set point was selected to provide adequate assurance that spurious reactor trips would not occur during normal operation. Table 7.4-1 lists the factors which make up the maximum overpower level of 118% based upon a trip set point of 109%.

308

TABLE 7.4-1

INSTRUMENTATION DRIFT AND CALORIMETRIC ERRORS
NUCLEAR OVERPOWER TRIP CHANNEL

| | Set Point and Error Allowances: (% of rated power) | Estimated Instrument Errors: (% of rated power) |
|---|---|---|
| Nominal Set Point | 109 | - |
| Calorimetric Error | 2 | 1.55 |
| Axial power distribution effects on total ion chamber current | 5 | 3 |
| Instrumentation channel drift and set point reproductibility | 2 | 1.0 |
| Maximum overpower trip point assuming all individual errors are simultaneously in the most adverse direction | 118 | - |

309

## 7.5 PROCESS INSTRUMENTATION

### 7.5.1 Design Bases

The non-nuclear process instrumentation measures temperatures, pressures, flows, and levels in the Reactor Coolant System, Steam System, Reactor Containment and Auxiliary Systems. Process variables required on a continuous basis for the startup, operation, and shutdown of the unit are indicated, recorded and controlled from the Control Room. The quantity and types of process instrumentation provided ensure safe and orderly operation of all systems and processes over the full operating range of the plant.

Certain controls which require a minimum of operator attention, or are only in use intermittently, are located on local control panels near the equipment to be controlled. Monitoring of the alarms of such control systems are provided in the Control Room.

Certain process variable indications for normal operation and post accident conditions are made available in the Control Room and the emergency response facilities through the Critical Function Monitoring System (CFMS).

### 7.5.2 System Design

Much of the process instrumentation provide din the plant has been described in the Reactor Control System, the Reactor Protection System and the Nuclear Instrumentation System descriptions (see Sections 7.2, 7.3 and 7.4, respectively). The most important instrumentation used to monitor and control the plant have been described in the above systems descriptions. The remaining portion of the process instrumentation is generally shown on the respective systems process flow diagrams.

Condensate pots and wet legs are used to prevent process temperatures from actually reaching the transmitters.

Reactor Vessel Level Indicating System (RVLIS)

The Reactor Vessel Level Indicating System (RVLIS) provides a means to monitor the water level in the reactor vessel during a postulated accident. It is designed to function under all normal, abnormal, accident and post-accident conditions concurrent with seismic events. The RVLIS consists of two redundant trains, with redundant power supplies, which automatically compensate for variations in fluid density as well as for the effects of reactor coolant pump operation.

The level instrumentation is divided into the full range ($\Delta_{PF}$) and the dynamic range ($\Delta_{PF}$) in order to measure level under all conditions. The full range gives level indication from the bottom of the reactor vessel to the top of the reactor head during natural circulation conditions. The dynamic range gives indication of reactor vessel liquid level for any combination of running RCP's. Comparison of indicated d/p against an algorithm derived $\Delta P$ gives a relative void content of the coolant in the core. (See Figure 7.5-2)

The RVLIS utilizes RCS penetrations to manual isolation valves. At the valves are sealed capillary impulse lines (two at the reactor head and two at the seal table) which transmit pressure measurements to d/p transmitters located outside the Containment Building in the in

the Primary Auxiliary Building. The capillary impulse lines are sealed at the RCS end and at the penetrations (inside Containment) with sensor bellows which serve as hydraulic couplers. The impulse lines extend through the Containment wall to hydraulic isolators which seal and isolate the lines as well as provide hydraulic coupling to capillary tubes going to the d/p transmitters. Inside the Containment Building, strap-on RTD's are utilized for vertical runs of impulse lines to correct the reference leg density contributions to the d/p measurement. (See Figure 7.5-2)

Engineered Safety Features

The following instrumentation ensures coverage of the effective operation of the engineered safety features:

Containment Pressure

The containment pressure is transmitted to the main control board for post accident monitoring. Six transmitters, two in each of three safety channels, are installed outside the containment to prevent potential missile damage. The pressure is indicated (all six measurement loops) on the main control board; the range is –5 psig to 75 psig.

The six measurement loops, monitoring containment pressure, reflect the effectiveness of engineered safety features.

Separate from the above, a continuous record of containment pressure is provided in a separate recorder panel in the Control Room. Two redundant and separately channeled safety related, Containment Building pressure measurements are transmitted to and recorded in the Control Room; their range is –5 psig to +200 psig. Each pressure measurement loop consists of a pressure transmitter, a pressure recorder and the necessary signal conditioning equipment, including a power supply, located in the Control Room. Each measurement loop is powered from a separate safety related 118 volts AC instrument bus. (See Section 5.5)

Containment Building Hydrogen Concentration

Indication of hydrogen in the Containment Building during and after a postulated accident is available from redundant sample conditioners and analyzers. The concentration is continually recorded by 2 recorders located in the Control Room.

Containment Building and Sump Water Level

There are measuring loops for monitoring water level in the Containment Sump, Recirculation Sump and the Containment Building. Each loop consists of a sensor and transmitter located in the Containment Building and a power supply and recorder in the Control Room.

In addition, to alert the operator in the event of a flooding incident, a reactor pit water level alarm provides indication in the Control Room; and a water level sensing probe and remote control unit provide containment sump overflow indication to the Control Room.

Refueling Water Storage Tank Level

Two redundant channels indicate that Safety Injection and Containment Spray Systems have removed water from the storage tank. One level indication and two low level alarms are transmitted from the tank to the control board.

Safety Injection Pumps Discharge Pressure

These channels show that the safety injection pumps are operating. The transmitters are outside the Containment.

Safety Injection System Flows

Flow indication is provided to the control board for the high and low head injection lines, the recirculation phase containment spray lines, and the spray additive rank outlet line.

Pump Energization

All pump motor power feed breakers indicate that they have closed by energizing indicatng lights on the control board.

Valve Position

All engineered safety features valves have position indication on the control board to show proper positioning of the valves. Air operated and solenoid operated valves are selected so as to move in a preferred direction on the loss of air or power. Motor-operated valves remain in the position they held at the time of loss of power to the motor.

Residual Heat Exchangers

Individual exit flows are indicated, plus combined inlet temperature and individual exit temperatures are recorded, on the control board to monitor operation of the residual heat exchangers.

Service Water

Individual service water pump flows are monitored through the use of an annubar flow measurement system. This system provides flow indication at the service water pump location.

Air Coolers

Local flow indication is provided outside containment for service water flow to each cooling unit. Abnormal flow alarms are provided in the Control Room. Service water common inlet temperatures, and all outlet temperatures are displayed at the critical function monitoring system (CFMS). A Control Room alarm is actuated if the flow is low coincident with a safety injection signal. The transmitters are outside the Reactor Containment. In addition, the exit flow is monitored for radiation and alarmed in the Control Room if high radiation should occur. This is a common monitor and the faulty cooler can be located by manually blocking the flow to each unit in turn with locally operated valves.

Alarms

Visual and audible alarms are provided to call attention to abnormal conditions. The alarms are of the individual acknowledgment type; that is, the operator must recognize and silence the audible alarm for each alarm point. For most control systems, the sensing device and circuits for the alarms are independent, or isolated from, the control devices.

312

In addition to the above, the following local instrumentation is available:

a) Containment spray test lines total flow
b) Safety injection test line pressure and flow

Monitoring Systems

A Safety Parameter Display System (SPDS) is provided to the Control Room which continuously displays information from which plant status can be assessed. Information on the following functions is provided:

a) Reactivity Control
b) Reactor core cooling and heat removal from the primary system
c) Reactor coolant system integrity
d) Radioactivity control
e) Containment conditions

The SPDS consists of the Critical Functions Monitoring System (CFMS) and the Qualified Safety Parameters Display System (QSPDS). The CFMS displays and alarms of critical safety functions (set of actions, which preserve integrity of one or more physical barriers against radiation) are indicated in the Control Room (CR) and the three emergency response facilities Technical Support Center (TSC), Emergency Operations Facility (EOF) and Alternate Emergency Operations Facility (AEOF). The CFMS is a redundant computer system not designed to seismic and electrical class 1E criteria. The QSPDS is a backup display system to the CFMS that is qualified to seismic and electrical class 1E standards.

The QSPDS design and display is based on NRC Regulatory Guide 1.97 criteria. The CFMS provides for historical data storage and retrieval capability (HDSR). The HDSR system will record, store, recall and display historical information either as graphs and trends or printed logs.

The CFMS/QSPDS receive signals from various plant equipment. The CFMS receives signals from safety related and non-safety related sources, and adequate electrical separation is maintained by use of fiber optic links.

In order to comply with the requirements of Regulatory Guide 1.97, additions to the original plant design parameters were made. Transmitters monitoring many process variables were installed and the CFMS is utilized to alarm and display these parameters. In some cases local indicators are also provided to facilitate local operation needs. Besides additions, replacement of existing components were made to upgrade them to meet the requirements.

7.5.3 System Evaluation

Redundant instrumentation has been provided for all inputs to the protective system and vital control circuits.

Where wide process variable ranges and precise control are required, both wide range and narrow range instrumentation is provided.

All electrical and electronic instrumentation required for safe and reliable operation is supplied from four redundant instrumentation buses.

7.5.4 Instrument Required

Table 7.5-1 identifies the instruments used to demonstrate compliance with NRC Regulatory Guide 1.97. Exemptions to compliance are noted in the table.

The Technical Specifications establish required actions and completion times for Regulatory Guide 1.97 Type A and Category 1 instrument channels.

In addition, inoperability of the following associated recorders is limited to 14 days: Containment Pressure, Containment Water Level, Recirculation Sump Water Level, Containment Hydrogen Monitor, Steam Generator Water level (Wide Range), RCS Pressure (Wide Range), Cold Leg Temperature (Wide Range), Hot Leg Temperature (Wide Range), Pressurizer Water Level, RCS Subcooling Monitor.

Surveillance requirements for Regulatory Guide 1.97 Type A and Category 1 instruments are established in the Technical Specifications. In addition, a Channel Operational Test is required, as follows, for alarms that are associated with Type A and Category 1 instruments, but which have no Regulatory Guide function:

- Main Steam Line Radiation (R62), Quarterly
- Gross Failed Fuel Detector (R63), Quarterly
- Containment Hydrogen Monitor, Monthly

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| 101A | A1 | Primary Coolant | Pressure, Reactor Coolant System, Loop 1 | P402 | J |
| 101B | A1 | Primary Coolant | Pressure, Reactor Coolant System, Loop 4 | P403 | J |
| 102A | A1 | Primary Coolant | Temperature, Hot Leg Loop No. 1 | T413A | P |
| 102B | A1 | Primary Coolant | Temperature, Hot Leg Loop No. 2 | T423A | P |
| 102C | A1 | Primary Coolant | Temperature, Hot Leg Loop No. 3 | T433A | P |
| 102D | A1 | Primary Coolant | Temperature, Hot Leg Loop No. 4 | T443A | P |
| 103A | A1 | Primary Coolant | Temperature, Cold Leg Loop No. 1 | T413B | P |
| 103B | A1 | Primary Coolant | Temperature, Cold Leg Loop No. 2 | T423B | P |
| 103C | A1 | Primary Coolant | Temperature, Cold Leg Loop No. 3 | T433B | P |
| 103D | A1 | Primary Coolant | Temperature, Cold Leg Loop No. 4 | T443B | P |
| 104A | A1 | Steam Generator 31 | Level, Wide Range | L417D | K |
| 104B | A1 | Steam Generator 31 | Level, Narrow Range | L417A | K |
| 104C | A1 | Steam Generator 31 | Level, Narrow Range | L417B | K |
| 104D | A1 | Steam Generator 31 | Level, Narrow Range | L417C | K |
| 104E | A1 | Steam Generator 32 | Level, Wide Range | L427D | K |
| 104F | A1 | Steam Generator 32 | Level, Narrow Range | L427A | K |
| 104G | A1 | Steam Generator 32 | Level, Narrow Range | L427B | K |
| 104H | A1 | Steam Generator 32 | Level, Narrow Range | L427C | K |
| 104I | A1 | Steam Generator 33 | Level, Wide Range | L437D | K |
| 104J | A1 | Steam Generator 33 | Level, Narrow Range | L437A | K |
| 104K | A1 | Steam Generator 33 | Level, Narrow Range | L437B | K |
| 104L | A1 | Steam Generator 33 | Level, Narrow Range | L437C | K |
| 104M | A1 | Steam Generator 34 | Level, Wide Range | L447D | K |
| 104N | A1 | Steam Generator 34 | Level, Narrow Range | L447A | K |
| 104O | A1 | Steam Generator 34 | Level, Narrow Range | L447B | K |
| 104P | A1 | Steam Generator 34 | Level, Narrow Range | L447C | K |
| 105A | A1 | Pressurizer | Level, Channel I | L459 | |
| 105B | A1 | Pressurizer | Level, Channel II | L460 | |
| 105C | A1 | Pressurizer | Level, Channel III | L461 | |



314

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| 106B | A1 | Containment | Wide Range Pressure, Channel I | P1421 | O |
| 106C | A1 | Containment | Wide Range Pressure, Channel II | P1422 | O |
| 107A | A1 | Steam Generator 31 | Pressure, Channel I | P419A | |
| 107B | A1 | Steam Generator 31 | Pressure, Channel II | P419B | |
| 107C | A1 | Steam Generator 31 | Pressure, Channel IV | P419C | |
| 107D | A1 | Steam Generator 32 | Pressure, Channel I | P429A | |
| 107E | A1 | Steam Generator 32 | Pressure, Channel II | P429B | |
| 107F | A1 | Steam Generator 32 | Pressure, Channel IV | P429C | |
| 107G | A1 | Steam Generator 33 | Pressure, Channel I | P439A | |
| 107H | A1 | Steam Generator 33 | Pressure, Channel II | P439B | |
| 107I | A1 | Steam Generator 33 | Pressure, Channel IV | P439C | |
| 107J | A1 | Steam Generator 34 | Pressure, Channel I | P449A | |
| 107K | A1 | Steam Generator 34 | Pressure, Channel II | P449B | |
| 107L | A1 | Steam Generator 34 | Pressure, Channel IV | P449C | |
| 108A | A1 | Refueling Water Storage Tank | Level, Alarm | L920 | N |
| 108B | A1 | Refueling Water Storage Tank | Level, Alarm | L921 | N |
| 109A | A1 | Containment | Water Level | L1253 | L |
| 109B | A1 | Containment | Water Level | L1254 | L |
| 111A | A1 | Containment | Radiation, Area, High Range | R25 | |
| 111B | A1 | Containment | Radiation, Area, High Range | R26 | |
| 112A | A1 | Secondary Cooling | Radiation, Main Steam | R62 | SS |
| 113A | A1 | Primary Coolant | Temperature, Core Exit | CE-T-*** | TT |
| 114A | A1 | Condensate Storage Tank Level | Water Level | L1128 | |
| 114B | A1 | Condensate Storage Tank Level | Water Level | L1128A | |
| 115A | A1 | Primary Coolant | Temperature, Degrees of RCS Subcooling | QSPDS-A | M |



315

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| 115B | A1 | Primary Coolant | Temperature, Degrees of RCS Subcooling | QSPDS-B | M |
| 201A | B1 | Neutron Flux Excore | Radiation, Intermediate Range Channel I | N38 | |
| 201B | B1 | Neutron Flux Excore | Radiation, Intermediate Range Channel II | N39 | |
| 202A | B3 | Control Rods | Position | N/A | |
| 203A | B3 | Primary Coolant | Sampling, Soluble Boron Concentration | N/A | Grab Sample |
| 204A | B3 | Primary Coolant | Temperature, Cold Leg, Loop No. 1 | T413B | P |
| 204B | B3 | Primary Coolant | Temperature, Cold Leg, Loop No. 2 | T423B | P |
| 204C | B3 | Primary Coolant | Temperature, Cold Leg, Loop No. 3 | T433B | P |
| 204D | B3 | Primary Coolant | Temperature, Cold Leg. Loop No. 4 | T433B | P |
| 205A | B1 | Primary Coolant | Temperature, Hot Leg, Loop No. 1 | T413A | P |
| 205B | B1 | Primary Coolant | Temperature, Hot Leg, Loop No. 2 | T423A | P |
| 205C | B1 | Primary Coolant | Temperature, Hot Leg, Loop No. 3 | T433A | P |
| 205D | B1 | Primary Coolant | Temperature, Hot Leg, Loop No. 4 | T443A | P |
| 206A | B1 | Primary Coolant | Temperature, Cold Leg, Loop No. 1 | T413B | P |
| 206B | B1 | Primary Coolant | Temperature, Cold Leg, Loop No. 2 | T423B | P |
| 206C | B1 | Primary Coolant | Temperature, Cold Leg, Loop No. 3 | T433B | P |
| 206D | B1 | Primary Coolant | Temperature, Cold Leg, Loop No. 4 | T443B | P |
| 207A | B1 | Primary Coolant | Pressure, Reactor Coolant System, Loop 1 | P402 | J |
| 207B | B1 | Primary Coolant | Pressure, Reactor Coolant System, Loop 4 | P403 | J |
| 208A | B3 | Primary Coolant | Temperature, Core Exit | CE-T-*** | TT |
| 209A | B1 | Primary Coolant | Level, Reactor | RVLIS TR-A & B | |
| 210A | B2 | Primary Coolant | Temperature, Degrees of Subcooling | QSPDS-A | |
| 210B | B2 | Primary Coolant | Temperature, Degrees of Subcooling | QSPDS-B | |
| 211A | B1 | Primary Coolant | Pressure, Reactor Coolant System, Loop 1 | P402 | J |
| 211B | B1 | Primary Coolant | Pressure, Reactor Coolant System, Loop 4 | P403 | J |
| 212C | B2 | Containment | Level, Containment Sump Water Channel I | L1255 | L |
| 212D | B2 | Containment | Level, Containment Sump Water Channel II | L1256 | L |
| 212E | B1 | Containment | Level, Wide Range Channel I | L1253 | L |



316

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| 212F | B1 | Containment | Level, Wide Range Channel II | L1254 | L |
| 212I | B2 | Containment | Level, Wide Range Redundant Channel: Recirculation Sump Level-Channel I | L1251 | L |
| 212J | B2 | Containment | Level, Wide Range Redundant Channel: Recirculation Sump Level-Channel II | L1252 | L |
| 213B | B1 | Containment | Pressure, Channel I | P1421 | O |
| 213C | B1 | Containment | Pressure, Channel II | P1422 | O |
| | | | | | |
| 214A | B1 | Containment | Position, Isolation valve | N/A | Y |
| 215B | B1 | Containment | Pressure, Channel I | P1421 | O |
| 215C | B1 | Containment | Pressure, Channel II | P1422 | O |
| 301A | C1 | Primary Coolant | Temperature, Core Exit | CE-T-*** | TT |
| 302A | C1 | Primary Coolant | Radiation, Radioactivity Concentration | R-63A&B | |
| 303A | C1 | Primary Coolant | Radiation, Gamma Spectrum | N/A | W |
| 304A | C1 | Primary Coolant | Pressure, Reactor Coolant System Loop 4 | P402 | J |
| 304B | C1 | Primary Coolant | Pressure, Reactor Coolant System Loop 1 | P403 | J |
| 305B | C1 | Containment | Pressure, Channel I | P1421 | O |
| 305C | C1 | Containment | Pressure, Channel II | P1422 | O |
| 306C | C2 | Containment | Level, Containment Sump Water Channel I | L1255 | L |
| 306D | C2 | Containment | Level, Containment Sump Water Channel II | L1256 | L |
| 306E | C1 | Containment | Level, Wide Range Channel I | L1253 | L |
| 306F | C1 | Containment | Level, Wide Range Channel II | L1254 | L |
| 306I | C1 | Containment | Level, Wide Range Redundant Channel: Recirculation Sump Level-Channel I | L1251 | L |
| 306J | C1 | Containment | Level, Wide Range Redundant Channel: Recirculation Sump Level-Channel II | L1252 | L |
| 307A | C3 | Containment | Radiation, Area | R25 | |
| 307B | C3 | Containment | Radiation, Area | R26 | |
| 308A | C3 | Cond Air Removal Sys | Radiation, Effluent Noble Gas | R15 | |



312

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| | | Exhaust | | | |
| 309A | C1 | Primary Coolant | Pressure, Reactor Coolant System, Loop 1 | P402 | J |
| 309B | C1 | Primary Coolant | Pressure, Reactor Coolant System, Loop 4 | P403 | J |
| 310B | C1 | Containment Air | Sampling, Hydrogen Concentration Channel I | HCMC-A | |
| 310C | C1 | Containment Air | Sampling, Hydrogen Concentration Channel II | HCMC-B | |
| 311B | C1 | Containment | Pressure, Channel I | P1421 | O |
| 311C | C1 | Containment | Pressure, Channel II | P1422 | O |
| 312A | C2 | Containment | Radiation, Effluent, Noble Gas, Penetration Area | R12 | AA |
| 314B | C2 | Penetration Area | Radiation, Area, Electrical Tunnel In Area of Electrical Penetration | N/A | BB |
| 314C | C2 | Penetration Area | Radiation, Area, 83' Personnel Airlock Area | N/A | BB |
| 314D | C2 | Penetration Area | Radiation, Area, Containment Purge Valve Area Between Containment & Fan House | N/A | BB |
| 314E | C2 | Penetration Area | Radiation, Area, 95' Personnel & Equipment Hatch Area | N/A | BB |
| 314F | C2 | Penetration Area | Radiation, Area, Fuel Transfer Area Between Containment & Fuel Storage Buildings | N/A | BB |
| 314G | C2 | Fuel Storage Building | Radiation, Area, Penetration Area, In Area of Fuel Transfer Tube | R5 | BB |
| 314H | C2 | PAB 34' FL EL | Radiation Area, Piping Tunnel In Area of Containment Sump Drain Pent | N/A | BB |
| 314J | C2 | PAB 54' FL EL | Radiation, Area, Piping Tunnel in Area of Piping Penetrations | N/A | BB |
| 401A | D2 | Residual Heat Removal | Flow Rate, Header 31 | F638 | |
| 401B | D2 | Residual Heat Removal | Flow Rate, Header 32 | F640 | |
| 401C | D2 | Residual Heat Removal | Flow Rate, Loop 4 | FT946A | |
| 401D | D2 | Residual Heat Removal | Flow Rate, Loop 3 | FT946B | |
| 401E | D2 | Residual Heat Removal | Flow Rate, Loop 2 | FT946C | |
| 401F | D2 | Residual Heat Removal | Flow Rate, Loop 1 | FT946D | |



318

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| 402A | D2 | Residual Heat Removal | Temperature, Heat Exchanger 31 Outlet | T639 | |
| 402B | D2 | Residual Heat Removal | Temperature, Heat Exchanger 32 Outlet | T641 | |
| 403A | D2 | Safety Injection | Level, Accumulator Tank 31 | L934A | Z |
| 304B | D2 | Safety Injection | Level, Accumulator Tank 32 | L934B | Z |
| 403C | D2 | Safety Injection | Level, Accumulator Tank 33 | L934C | Z |
| 403D | D2 | Safety Injection | Level, Accumulator Tank 34 | L934D | Z |
| 403E | D2 | Safety Injection | Pressure, Accumulator Tank 31 | P937A | Z |
| 403F | D2 | Safety Injection | Pressure, Accumulator Tank 32 | P937B | Z |
| 403G | D2 | Safety Injection | Pressure, Accumulator Tank 33 | P937C | Z |
| 403H | D2 | Safety Injection | Pressure, Accumulator Tank 34 | P937D | Z |
| 404A | D2 | Safety Injection | Pressure, Accumulator Tank 31 Isolation Valve 894A | N/A | HH |
| 404B | D2 | Safety Injection | Pressure, Accumulator Tank 32 Isolation Valve 894B | N/A | HH |
| 404C | D2 | Safety Injection | Pressure, Accumulator Tank 33 Isolation Valve 894C | N/A | HH |
| 404D | D2 | Safety Injection | Pressure, Accumulator Tank 34 Isolation Valve 894D | N/A | HH |
| 405A | D2 | Safety Injection | Flow, Boric Acid Charging | F128 | H |
| 406A | D2 | Safety Injection | Flow, High Head, Cold Leg Loop I | F926 | |
| 406B | D2 | Safety Injection | Flow, High Head, Cold Leg Loop I | F924A | |
| 406C | D2 | Safety Injection | Flow, High Head, Cold Leg Loop 2 | F981 | |
| 406D | D2 | Safety Injection | Flow, High Speed, Cold Leg Loop 2 | F925 | |
| 406E | D2 | Safety Injection | Flow, High Speed, Cold Leg Loop 3 | F980 | |
| 406F | D2 | Safety Injection | Flow, High Speed, Cold Leg Loop 3 | F926A | |
| 406G | D2 | Safety Injection | Flow, High Speed, Cold Leg Loop 4 | F982 | |
| 406H | D2 | Safety Injection | Flow, High Speed, Cold Leg Loop 4 | F927 | |
| 407A | D2 | Safety Injection | Flow, Low Head | F638 | |



349

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| 407B | D2 | Safety Injection | Flow, Low Head | F640 | |
| 408A | D2 | Safety Injection | Level, Refueling Water Storage Tank | L920 | |
| 409A | D3 | Primary Coolant | Status, Reactor Coolant Pump 31 | N/A | |
| 409B | D3 | Primary Coolant | Status, Reactor Coolant Pump 32 | N/A | |
| 409C | D3 | Primary Coolant | Status, Reactor Coolant Pump 33 | N/A | |
| 409D | D3 | Primary Coolant | Status, Reactor Coolant Pump 34 | N/A | |
| 410A | D2 | Primary Coolant | Position, Safety Relief Valve, Power Operated Relief Valve 455C | N/A | Acoustical Monitor At Valve |
| 410B | D2 | Primary Coolant | Position, Safety Relief Valve, Power Operated Relief Valve 456 | N/A | Acoustical Monitor At Valve |
| 410C | D2 | Primary Coolant | Position, Safety Relief Valve, ASME Code Safety Valve 464 | N/A | Acoustical Monitor At Valve |
| 410D | D2 | Primary Coolant | Position, Safety Relief Valve, ASME Code Safety Valve 466 | N/A | Acoustical Monitor At Valve |
| 410E | D2 | Primary Coolant | Position, Safety Relief Valve, ASME Code Safety Valve 468 | N/A | Acoustical Monitor At Valve |
| 411A | D1 | Primary Coolant | Level, Pressurizer Channel I | L459 | |
| 411B | D1 | Primary Coolant | Level, Pressurizer Channel II | L460 | |
| 411C | D1 | Primary Coolant | Level, Pressurizer Channel III | L461 | |
| 412A | D2 | Primary Coolant | Status, Pressurizer Heater – Control Group | N/A | U |
| 412B | D2 | Primary Coolant | Status, Pressurizer Heater – Back-up Group 31 | N/A | U |
| 412C | D2 | Primary Coolant | Status, Pressurizer Heater – Back-up Group 32 | N/A | U |
| 412D | D2 | Primary Coolant | Status, Pressurizer Heater – Back-up Group 33 | N/A | U |
| 413A | D3 | Primary Coolant | Level, Pressurizer Relief Tank 31 | L470 | |



320

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| 414A | D3 | Primary Coolant | Temperature, Pressurizer Relief Tank 31 | T471 | |
| 415A | D3 | Primary Coolant | Pressure, Pressurizer Relief Tank 31 | P472 | |
| 416A | D1 | Secondary Cooling | Level, Steam Generator 31 | L417D | K |
| 416B | D1 | Secondary Cooling | Level, Steam Generator 32 | L427D | K |
| 416C | D1 | Secondary Cooling | Level, Steam Generator 33 | L437D | K |
| 416D | D1 | Secondary Cooling | Level, Steam Generator 34 | L447D | K |
| 417A | D2 | Secondary Cooling | Pressure, Steam Generator 31, Channel I | P419A | |
| 417B | D2 | Secondary Cooling | Pressure, Steam Generator 32, Channel I | P429A | |
| 417C | D2 | Secondary Cooling | Pressure, Steam Generator 33, Channel I | P439A | |
| 417D | D2 | Secondary Cooling | Pressure, Steam Generator 34, Channel I | P449A | |
| 418A | D2 | Secondary Cooling | Flow, Main Steam From Steam Generator 31 | F419A&B | |
| 418B | D2 | Secondary Cooling | Flow, Main Steam From Steam Generator 32 | F429A&B | |
| 418C | D2 | Secondary Cooling | Flow, Main steam From Steam Generator 33 | F439A&B | |
| 418D | D2 | Secondary Cooling | Flow, Main Steam From Steam Generator 34 | F449A&B | |
| 419A | D3 | Secondary Cooling | Flow, Main Feedwater To Steam Generator 31 | F418A&B | |
| 419B | D3 | Secondary Cooling | Flow, Main Feedwater To Steam Generator 32 | F428A&B | |
| 419C | D3 | Secondary Cooling | Flow, Main Feedwater To Steam Generator 33 | F438A&B | |
| 419D | D3 | Secondary Cooling | Flow, Main Feedwater To Steam Generator 34 | F448A&B | |
| 420A | D2 | Secondary Cooling | Flow, Auxiliary Feedwater To Steam Generator 31 | F1200R | |
| 420B | D2 | Secondary Cooling | Flow, Auxiliary Feedwater To Steam Generator 32 | F1201R | |
| 420C | D2 | Secondary Cooling | Flow, Auxiliary Feedwater To Steam Generator 33 | F1202R | |
| 420D | D2 | Secondary Cooling | Flow, Auxiliary Feedwater To Steam Generator 34 | F1203R | |
| 421A | D1 | Secondary Cooling | Level, Condensate Storage Tank Water | L1128 | G |
| 421B | D1 | Secondary Cooling | Level, Condensate Storage Tank Water | L1128A | G |
| 422A | D2 | Containment | Flow, Spray From Residual Heat Removal Heat Exchanger 31 | F945B | II |
| 422B | D2 | Containment | Flow, Spray From Residual Heat Removal Heat Exchanger 32 | F945A | II |
| 423A | D2 | Containment | Flow, Heat Removal By System-Service Water | F1121 | |



321

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| | | | RCFC 31 | | |
| 423B | D2 | Containment | Flow, Heat Removal By system-Service Water RCFC 32 | F1122 | |
| 423C | D2 | Containment | Flow, Heat Removal By System-Service Water RCFC 33 | F1123 | |
| 423D | D2 | Containment | Flow, Heat Removal By System-Service Water RECF 34 | F1124 | |
| 423E | D2 | Containment | Flow, Heat Removal By System-Service Water RCFC 35 | F1125 | |
| 423F | D2 | Containment | Temperature, Heat Removal By System-Service Water Diff RCFC 31 | T-1415-1 | |
| 423G | D2 | Containment | Temperature, Heat Removal By System-Service Water Diff RCFC 32 | T-1415-2 | |
| 423H | D2 | Containment | Temperature, Heat Removal By System-Service Water Diff RCFC 33 | T-1415-3 | |
| 423J | D2 | Containment | Temperature, Heat Removal By-System-Service Water Diff RCFC 34 | T-1415-4 | |
| 423K | D2 | Containment | Temperature, Heat Removal By System-Service Water Diff RCFC 35 | T-1415-5 | |
| 424A | D2 | Containment | Temperature, Atmosphere | T1203 | |
| 425A | D2 | Containment | Temperature, Sump Water | NONE | I |
| 426A | D2 | Chemical & Volume Control | Flow, Make-up In | F128 | |
| 427A | D2 | Chemical & Volume Control | Flow, Letdown Out | F134 | B |
| 428A | D2 | Chemical & Volume Control | Level, Volume Control Tank | L112 | C |
| 429A | D2 | Component Cooling | Temperature, Component Cooling Heat Exchanger 31 Output | T602A | D |

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| 429B | D2 | Component Cooling | Temperature, Component Cooling Heat Exchanger 32 Output | T602B | D |
| 430A | D2 | Component Cooling | Flow, Component Cooling Heat Exchanger 31 Output | F601A | E |
| 430B | D2 | Component Cooling | Flow, Component Cooling Heat Exchanger 32 Output | F601B | E |
| 431A | D3 | Radwaste | Level, High-Level Radioactive Waste Hold-up Tank 31 | L1001 | |
| 431B | D3 | Radwaste | Level, High-Level Radioactive Waste Hold-up Tank 32 (3HBT01A) | L168 | JJ |
| 431C | D3 | Radwaste | Level, High-Level Radioactive Waste Hold-up Tank 33 (3HBT01B) | L170 | JJ |
| 432A | D3 | Radwaste | Pressure, Large Radioactive Gas Decay Tank 31 | P1036 | KK |
| 432B | D3 | Radwaste | Pressure, Large Radioactive Gas Decay Tank 32 | P1037 | KK |
| 432C | D3 | Radwaste | Pressure, Large Radioactive Gas Decay Tank 33 | P1038 | KK |
| 432D | D3 | Radwaste | Pressure, Large Radioactive Gas Decay Tank 34 | P1039 | KK |
| 432E | D3 | Radwaste | Pressure, Small Radioactive Gas Decay Tank 31 | P1052 | KK |
| 432F | D3 | Radwaste | Pressure, Small Radioactive Gas Decay Tank 32 | P1053 | KK |
| 432G | D3 | Radwaste | Pressure, Small Radioactive Gas Decay Tank 33 | P1054 | KK |
| 432H | D3 | Radwaste | Pressure, Small Radioactive Gas Decay Tank 34 | P1055 | KK |
| 432J | D3 | Radwaste | Pressure, Small Radioactive Gas Decay Tank 35 | P1056 | KK |
| 432K | D3 | Radwaste | Pressure, Small Radioactive Gas Decay Tank 36 | P1057 | KK |
| 433A | D2 | Ventilation | Position, Reactor Containment Fan Cooler 31 Damper A & B | N/A | GG |
| 433B | D2 | Ventilation | Position, Reactor Containment Fan Cooler 31 Damper A & B | N/A | GG |
| 433C | D2 | Ventilation | Position, Reactor Containment Fan Cooler 31 Damper D & Blow-in Door | N/A | GG |
| 433D | D2 | Ventilation | Position, Reactor Containment Fan Cooler 32 | N/A | GG |



323

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| | | | Damper A & B | | |
| 433E | D2 | Ventilation | Position, Containment Fan Cooler 32 Damper C | N/A | GG |
| 433F | D2 | Ventilation | Position, Reactor Containment Fan Cooler 32 Damper D & Blow-in Door | N/A | GG |
| 433G | D2 | Ventilation | Position, Reactor Containment Fan Cooler 33 Damper A & B | N/A | GG |
| 433H | D2 | Ventilation | Position, Reactor Containment Fan Cooler 33 Damper C | N/A | GG |
| 433J | D2 | Ventilation | Position, Reactor Containment Fan Cooler 33 Damper D & Blow-in Door | N/A | GG |
| 433K | D2 | Ventilation | Position, Reactor Containment Fan Cooler 34 Damper A & B | N/A | GG |
| 433L | D2 | Ventilation | Position, Reactor Containment Fan Cooler 34 Damper C | N/A | GG |
| 433M | D2 | Ventilation | Position, Reactor Containment Fan cooler 34 Damper D & Blow-in Door | N/A | GG |
| 433N | D2 | Ventilation | Position, Reactor Containment Fan Cooler 35 Damper A & B | N/A | GG |
| 433P | D2 | Ventilation | Position, Reactor Containment Fan Cooler 35 Damper C | N/A | GG |
| 433R | D2 | Ventilation | Position, Reactor Containment Fan Cooler 35 Damper D & Blow-in Door | N/A | GG |
| 433S | D2 | Ventilation | Position, Fuel Storage Building Forced Air Unit 31 Emergency Damper | N/A | GG |
| 433T | D2 | Ventilation | Position, Fuel Storage Building Forced Air Unit 32 Emergency Damper | N/A | GG |
| 433U | D2 | Ventilation | Position, Fuel Storage Building Normal Airflow Top Damper | N/A | GG |
| 433V | D2 | Ventilation | Position, Fuel Storage Building Normal Airflow Bottom Damper | N/A | GG |

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| 433W | D2 | Ventilation | Position, Fuel Storage Building Emergency Airflow Filter Intake Damper | N/A | GG |
| 433X | D2 | Ventilation | Position, Fuel Storage Building Emergency Airflow Filter Exhaust Damper | N/A | GG |
| 433Y | D2 | Ventilation | Position, Primary Auxiliary Building Exhaust Charcoal Damper – Face | N/A | GG |
| 433Z | D2 | Ventilation | Position, Primary Auxiliary Building Exhaust Charcoal Damper – Bypass | N/A | GG |
| 434A | D2 | Emergency Power | Current, AC Bus 31 | N/A | |
| 434B | D2 | Emergency Power | Current, AC Bus 32 | N/A | |
| 434C | D2 | Emergency Power | Current, AC Bus 33 | N/A | |
| 434D | D2 | Emergency Power | Current, AC Bus 34 | N/A | |
| 434E | D2 | Emergency Power | Voltage, AC Bus 31 | N/A | |
| 434F | D2 | Emergency Power | Voltage, AC Bus 32 | N/A | |
| 434G | D2 | Emergency Power | Voltage, AC Bus 33 | N/A | |
| 434H | D2 | Emergency Power | Voltage, AC Bus 34 | N/A | |
| 434I | D2 | Emergency Power | Current, DC Bus 31 | N/A | F |
| 434J | D2 | Emergency Power | Current, DC Bus 32 | N/A | F |
| 434K | D2 | Emergency Power | Current, DC Bus 33 | N/A | F |
| 434L | D2 | Emergency Power | Current, DC Bus 34 | N/A | F |
| 434M | D2 | Emergency Power | Voltage, DC Bus 31 | N/A | |
| 434N | D2 | Emergency Power | Voltage, DC Bus 32 | N/A | |
| 434O | D2 | Emergency Power | Voltage, DC Bus 33 | N/A | |
| 434P | D2 | Emergency Power | Voltage, DC Bus 34 | N/A | |
| 434Q | D2 | Emergency Power | Current, Diesel 31 | N/A | |
| 434R | D2 | Emergency Power | Current, Diesel 32 | N/A | |
| 434S | D2 | Emergency Power | Current, Diesel 33 | N/A | |
| 434T | D2 | Emergency Power | Voltage, Diesel 31 | N/A | |
| 434U | D2 | Emergency Power | Voltage, Diesel 32 | N/A | |

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| 434V | D2 | Emergency Power | Voltage, Diesel 33 | N/A | |
| 434W | D2 | Emergency Air Supply | Pressure, Instrument Air Receiver Tank | P1207 | |
| 434X | D2 | Emergency Air Supply | Pressure, Diesel 31 Starting Air Receiver Tank | N/A | |
| 434Y | D2 | Emergency Air Supply | Pressure, Diesel 32 Starting Air Receiver Tank | N/A | |
| 434Z | D2 | Emergency Air Supply | Pressure, Diesel 33 Starting Air Receiver Tank | N/A | |
| 501A | E1 | Containment | Radiation, Area, High Range | R25 | |
| 501B | E1 | Containment | Radiation, Area, High Range | R26 | |
| 502A | E3 | Central Control Room | Radiation, Area | R1 | MM,CC,X |
| 502B | E3 | PAB 80' | Radiation, Area, Charging Pump Room | R4 | DD |
| 502C | E3 | Fuel Storage Building | Radiation, Area | R5 | |
| 502D | E3 | PAB 55' | Radiation, Area, Sampling Room (North Wall) | R6 | X |
| 502E | E2 | Containment | Radiation, Area, (AT Seal Table) In-core Instrument Room | R7 | X, DD |
| 502F | E2 | PAB 55' | Radiation, Area, Drumming Station | R8 | X, DD |
| 502G | E2 | Aux Boiler Feed Pump Bldg | Radiation, Area, (West Wall Opposite Main Steam Penetrations 31 & 32) | NONE | X |
| 502H | E2 | PAB 55' | Radiation, Area, On Column Across From Sample Room | R64 | |
| 502J | E2 | PAB 73' | Radiation, Area, Entrance Way To Volume Control Tank | N/A | X |
| 502K | E2 | PAB 73' | Radiation, Area, Hall Next To NPO Office | R65 | |
| 502L | E2 | PAB 41' | Radiation, Area, South Wall Area Of Refueling Water Purification Pumps | N/A | X |
| 502M | E2 | PAB 41' | Radiation, Area, Hall On Column Next To Containment Spray Pumps | N/A | X |
| 502N | E2 | PAB 34' | Radiation, Area, Hall Near Entry To Safety Injection Pumps | R66 | |



326

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| 502P | E2 | PAB 41' | Radiation, Area, Pipe Tunnel In Area Of Chemistry Post Accident Sampling Station | R67 | |
| 502Q | E2 | PAB 15' | Radiation, Area, On North Wall Adjacent To RHR Valve Gallery | R68 | |
| 502R | E2 | RAB 15' | Radiation, Area, Hall On Wall At Entry To Filter Cell | N/A | X |
| 502S | E2 | PAB 54' | Radiation, Area, Within The Doorway On The Wall, Pipe Penetration | R69 | |
| 502T | E2 | PAB 67' | Radiation, Area, Above Pipe Penn In Area Of Hydrogen Recombiner Panels | N/A | X |
| 502U | E2 | Fan Building 92' | Radiation, Area, In Area Of 4 Channel Iodine Monitors | R70 | |
| 502V | E2 | Fan Building 72' | Radiation, Area, Outside Plenum In Area Of Differential Pressure Instruments | R70 | |
| 503A | E2 | Containment | Radiation, Effluent, Noble Gas | R27 | Via Plant Vent |
| 504A | E2 | Reactor Shield Building Annulus | Radiation, Effluent, Noble Gas | N/A | |
| 505A | E2 | Auxiliary Building | Radiation, Effluent, Noble Gas, Or Others Containing Primary System Gases | R27 | Via Plant Vent |
| 506A | E2 | Cond Air Removal Sys Exhaust | Radiation, Effluent, Noble Gas | R15 | NN |
| 506B | E2 | Cond Air Removal Sys Exhaust | Radiation, Effluent, Noble Gas – Flow Rate | R15 | |
| 507 A | E2 | Common Plant Vent | Radiation, Effluent, Noble Gas | R27 | SS |
| 507B | E2 | Common Plant Vent | Radiation, Effluent, Flow Rate | R27 | SS |
| 508A | E2 | Steam Generator | Radiation, Effluent, Noble Gas From Safety Relief Valves Or Atm Dump Valves | R62 | FF |
| 509A | E2 | Admin Bldg Exhaust Vent | Radiation, Effluent, Noble Gas From 4th Floor | R46 | OO, CC |



327

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| 509B | E2 | Admin Bldg Exhaust Vent | Radiation, Effluent, Flow Rate, 4th Floor | NONE | OO |
| 509C | E2 | Radioactive Machine Shop Exhaust Vent | Radiation, Effluent, Noble Gas | R59 | |
| 509D | E2 | Radioactive Machine Shop Exhaust Vent | Radiation, Effluent, Flow Rate | FT-1776 | |
| 509E | E2 | Steam Generator Blowdown | Radiation, Effluent | R19 | |
| 509F | E2 | Steam Generator Blowdown | Radiation, Effluent, Flow Rate | F538 | |
| 510A | E3 | Common Plant Vent | Radiation, Effluent, Particulates | N/A | EE, SS |
| 510B | E3 | Common Plant Vent | Radiation,, Effluent, Halogens | N/A | EE, SS |
| 510C | E3 | Common Plant Vent | Radiation, Effluent, Flow Rate | R27 | |
| 510D | E3 | Admin Bldg Exhaust Vent | Radiation, Effluent, Particulates From The 4th Floor | N/A | DD, OO |
| 510E | E3 | Admin Bldg Exhaust Vent | Radiation, Effluent, Halogens From The 4th Floor | N/A | DD, OO |
| 510F | E3 | Admin Bldg Exhaust Vent | Radiation, Effluent, Flow Rate, 4th Floor | NONE | DD, OO |
| 510G | E3 | Radioactive Machine Shop Exhaust Vent | Radiation, Effluent, Particulates | N/A | CC |
| 510H | E3 | Radioactive machine shop exhaust vent | Radiation, Effluent, Halogens | NONE | CC |
| 510J | E3 | Radioactive machine shop exhaust vent | Radiation, Effluent, Flow Rate | FT-1776 | |
| 511A | E3 | Environs | Radiation, Exposure Rate | N/A | RR |
| 512A | E3 | Environs | Radiation, airborne radiohalogens and particulates | N/A | portable instrum. |
| 513A | E3 | Environs | Radiation, photons | N/A | portable instrum. |
| 513B | E3 | Environs | Radiation, beta and low energy photons | N/A | portable instrum. |

TABLE 7.5-1
Regulatory Guide 1.97 Instruments Required

| REG GUIDE 1.97 | | STATUS OF COMPLIANCE | | | |
|---|---|---|---|---|---|
| INDEX | TYPE CAT | VARIABLE ONE | VARIABLE TWO | INST LOOP | NOTES |
| 514A | E3 | Environs | Radioactivity, multi channel gamma-ray spectrometer | N/A | |
| 515A | E3 | Meteorological | Met, wind direction | N/A | |
| 516A | E3 | Meteorological | Met, wind speed | N/A | |
| 517A | E3 | Meteorological | Met, atmospheric stability | N/A | |
| 518A | E3 | Sampling | Primary coolant and containment sump water analysis – gross activity | N/A | W,R |
| 518B | E3 | Sampling | Primary coolant and containment sump water analysis – gamma spectrum | N/A | W,R |
| 518C | E3 | Sampling | Primary coolant and containment sump water analysis – boron content | N/A | W,R |



329

**Table 7.5-1**

**Regulatory Guide 1.97 Instruments Required**
**NOTES**

General Notes that apply to all items have an * as an identifier.

**NOTE A**: DELETED

**NOTE B**: The letdown flow is controlled by opening a remote operated valve, which allows flow through fixed orifice plates. The maximum CVCS letdown flow allowed administratively is limited to 120 gpm. It is the Authority's position that the indicated range (0-125 gpm) is adequate.

**NOTE C**: The existing level (18% to 82%) transmitter range is adequate. The modification necessary to obtain the additional level (0%-100%) required by 1.97 is not warranted based on manrem exposure and cost versus benefit.

**NOTE D**: The existing range indication for component cooling heat exchanger temperature is adequate for all modes of normal operation of off-normal modes of operation. The temperature of the component cooling system to date has not decreased below the existing range of 50°F. In addition, in the event of a major accident the temperature would be expected to increase as opposed to decrease, further assuring that the temperature would not decrease below the low range of the temperature system.

**NOTE E**: The existing range indication for component cooling heat exchanger flow is adequate for all modes of normal operation or off-normal modes of operation. The component cooling flow indication during normal operation may decrease below the existing range however; this condition does not cause any concern warranting a modification. The pump can be assured that it is functioning via low pressure and pump breaker status alarms. The components that are being cooled have local flow devices that are used to regulate the flow; therefore, minimum pump flow conditions can be met. In addition, in the event of a major accident, the flow would increase as opposed to decrease.

**NOTE F**: It is the Authority's position that sufficient indication to D.C. bus status is provided to the operators such that during post accident conditions, the operators will be aware of the operability of the D.C. buses.

**NOTE G**: Condensate storage tank level is currently monitored by two-(2) independent qualified transmitters. Diverse indication of CST level can be derived by auxiliary feedwater suction pressure indication. It is the Authority's position that the existing monitoring of CST level complies with the requirements of Regulatory Guide 1.97.

**NOTE H**: Boric acid flow to the RCS is monitored by the high-pressure injection (HPI) flow transmitters. Refer to index number 406 A-H which meets Reg. Guide 1.97 requirements.



330

**NOTE I**: Based on conversations with the NRC staff, the intent of this variable may be satisfied by the indication of several other variables. IP-3 has indication of RHR outlet temperature, containment spray flow and containment temperature which provides adequate indication of containment heat removal capability.

**NOTE J**: Adequate diverse measurement to PT-402 and PT-403 is obtained from pressure transmitters used to monitor pressurizer pressure (PT-455, 456, 457 and 474) for the range of 1700-2500 psig. Additionally, R.C.S. pressure, 0-3000 psig is indicated on a pressure gauge located in an area accessible to plant operators.

**NOTE K**: Each Steam Generator contains four (4) transmitters to indicate steam generator water level Three (3) transmitters per steam generator indicate narrow range level which is a span that begins at the top of the tube bundles to the moisture separator. The remaining level transmitter covers the span from the bottom tube sheet up to the moisture separator. Based on above, diversity exists from the top portion of the steam generator. Two (2) auxiliary feedwater flow indicators provide a diverse indication for the steam generator. In addition, since two of our four steam generators are required for heat removal, redundant wide range level for each generator is deemed not necessary.

**NOTE L**: Two (2) redundant level transmitters (LT-1253 & 1254) provide containment water level indication to the Central Control Room (CCR) operators. In addition, the containment sump and recirculation sump each contain (2) qualified level transmitters. The refueling water storage tank provides a diverse measurement for the containment water level.

**NOTE M**: Diversity is met via a third system which records saturation pressure margin and also use of steam tables.

**NOTE N**: Containment water level provides a diverse method to determine refueling water storage tank level.

**NOTE O**: Additional Containment pressure instrumentation exists (PT 948A, B & C and PT 949A, B & C) to provide a diverse means of establishing containment pressure.

**NOTE P**: Redundancy for the Hot Leg Reactor Coolant Temperature will be by the use of the core exit thermocouples (Diverse Variable). Redundancy for the Cold Leg Reactor Coolant Temperature is provided by the steamline pressure instrument PT 419 A, B & C; PT 429 A, B, & C; PT 439 A, B, & C and PT 449 A, B, & C (Diverse Variable).

**NOTE Q**: DELETED

**NOTE R**: DELETED

**NOTE S***: On March 4, 1983, the NRC conducted a workshop in Chicago, Illinois in order to clarify the technical requirement of NUREG-0737, Supplement I. The handout distributed by the NRC at this workshop states that with respect to seismic qualification requirement for operating reactors, it will suffice to state that instrumentation systems comply with the seismic qualification program which was the basis for plant licensing. Accordingly, the seismic requirement is indicated



331

in Enclosure B as being satisfied if that instrumentation complies with the licensing basis for seismic qualification. [GENERAL NOTE]

**NOTE T***: As noted in Regulatory Guide 1.97, Revision 3, Category 1 and 2 instrumentation should be qualified in accordance with Regulatory Guide 1.89, "Qualification of Class 1E Equipment for Nuclear Power Plants," and the methodology described in NUREG-0588, "Interim Staff Position on Environmental Qualification of Safety-Related Electrical Equipment." Enclosure B reflects this requirement for all Category 1 and 2 instrumentation. However, certain Category 1 and 2 instrumentation are located in mild post-accident environments and therefore are not within the scope of Regulatory Guide 1.89. For the sake of convenience, the Category 1 and 2 instrumentation located in a mild post-accident environment are noted as meeting Environmental Qualification (E.Q.) requirement. Hence, that instrumentation noted in Enclosure B as satisfying the E.Q. requirement either satisfy the requirements of 10 CFR 50.49 or are located in a mild post-accident environment.

**NOTE U**: Since the purpose of Pressurizer Heater Status is to ensure that they do not overload a diesel, adequate diesel generator loading information is available to the operators. The heaters are supplied by a safety related electrical bus and are stripped from that bus in the event of a Safety Injection Signal. They must be manually placed in service by the control room operator and procedures are in place that provide the guidance to ensure the diesels are not overloaded.

In addition, heater electrical breaker status lights are available. The pressurizer pressure and temperature response also provides verification that the heaters are operational.

**NOTE V**: DELETED

**NOTE W**: The Authority concurred with the NRC approach to post-accident sampling capability review. The deviations are beyond the scope of the Regulatory Guide 1.97 submittal and are best addressed via our submittal to NuReg-0737, Item II.B.3

**NOTE X**: Portable survey meters are the primary source of data on the radiation exposure rates inside buildings. These portable instruments are used to 1) verify the indication of the existing installed radiation monitors, and 2) determine exposure rates where there are no installed radiation monitors. It is Entergy's opinion that the portable survey meters meet the intent of the Guide.

**NOTE Y**: The automatic containment isolation valves at the facility meet all of the requirements of the Regulatory Guide on position indication. Non-automatic containment isolation valves are not provided with position indication. Valves that are considered essential and non-automatic are maintained in the open position and are closed after the initial phases of an accident. Approved emergency procedures are utilized to control the closing of these valves. Non-essential

containment isolation valves are maintained in the closed position and may be opened, if necessary, for plant operation and for only as long as necessary to perform the intended function, as required by Indian Point 3 Technical Specifications. These valves are additionally administratively controlled in the following manner:

1. Shift Manager approval for opening a non-automatic containment isolation valve is required.
2. An operator must be dedicated to the operation of these valves as long as they are in the open position.
3. Operator must have communications established with the Central Control Room, and
4. Operators first response to any emergency condition while the valve is open is to insure that the valve is returned to the closed position.

**NOTE Z**: Since the accumulators will discharge immediately when RCS pressure drops below accumulation pressure, these variables are unnecessary following an accident. Since power to the isolation valves is locked out at the circuit breaker, the operator would not be able to utilize these variables for manual actions, except for events in which the RCS pressure is decreasing very slowly. For such events, the present indicators are expected to function properly. Letter from NRC (N. F. Conicella) to R. Beedle, dated 9/28/92, entitled "REGULATORY GUIDE 1.97 – INSTRUMENTATION TO FOLLOW THE COURSE OF AN ACCIDENT FOR INDIAN POINT GENERATING UNIT NO. 3 (TAC No. M51099)", relaxed the requirement for Accumulator Pressure and Level Instrumentation and deleted the commitment for upgrading Accumulator Pressure and Level Instrumentation.

**NOTE AA**: The original radiation monitor used to monitor containment effluent radioactivity (R-12) is located in a non-harsh environmental area. Therefore, the environmental qualification requirements of the regulatory guide are satisfied. The combination of R-12 and an additional environmentally qualified effluent radiation monitor (R-27) sufficiently meets the range requirements of the Regulatory Guide.

**NOTE BB**: Radiation exposure rates inside buildings or areas in direct contact with primary containment where penetrations and hatches are located can be sufficiently monitored by portable radiation monitoring detectors.

**NOTE CC**: The existing sampler or radiation monitors for these areas do not meet the range requirements of the Regulatory Guide, however, it is Entergy's position that the indicated range is sufficient for the highest levels that are postulated for these areas.

**NOTE DD**: The existing area radiation monitors for these areas do not meet the range requirements of the Regulatory Guide, however, it is Entergy's position that these areas need not be monitored for the mitigation of an accident.



33

**NOTE EE**: To accommodate the range requirements of these radiation detectors, Entergy will use the Post Accident Sampling System.

**NOTE FF**: The plant computer will record the steam release duration and mass flow rate.

**NOTE GG**: Damper indication status is provided via red-green indicating lamps in the control room. The lamps are illuminated by a single limit switch, which is toggled when the damper is in the opened or closed position.

The Containment Fan Cooler units are provided with flow switches, which will cause an annunciation in the control room if low flow exists. In addition, a Weir system exists to quantify the cooling and condensing features of the ventilation unit.

Since failure of dampers are rare and it is improbable that the limit switch or some diverse variable would not detect the failure, it is Entergy's position that no modifications are warranted.

**NOTE HH**: The white lights used to satisfy Index 404A, B, C, and D are on when the valves are fully open and off when not fully open. These lights are always operable.

The valves are opened and the power and control circuits are de-energized when the RCS pressure is above 1000 psi. When these circuits are energized, each valve has red and green indicator lights which tell the operator whether the valve is full open, full closed or at some intermediate position.

**NOTE II**: The containment spray system consists of 4 spray headers. Two headers are used during the initial phase of the accident and the other two headers are used later in the accident. Manual operator action based on spray system flow rates is required in the later phase of the accident. As such, the spray flow indications described in Enclosure B are provided by the two headers used later in the accident only.

**NOTE JJ**: The existing level represents approximately 94% of the tank range. Since the tanks are horizontal cylindrical, the level actually monitors greater than 94% of its volume. These tanks are back up to 31 Waste Hold-Up tanks.

**NOTE KK**: The range that is required by the Guide, 0 to 165 psig, exceeds the tank design pressure and the tank safety valve setting, i.e., 150 psig. As additional status of tank pressure, an alarm is actuated when tank pressure reaches 110 psig. It is therefore concluded that the actual range of tank pressure is acceptable and meets the intent of the Regulatory Guide.

**NOTE LL**: DELETED – Monitor R-10 has been removed from the plant.

**NOTE MM**: The control room monitor's range is considered adequate. The operators would evacuate the control room prior to fields reaching the upper range prescribed in Reg. Guide 1.97.

**NOTE NN**: This possible atmospheric release point is designed to divert into the containment at relatively low levels. In addition, prior to reaching 1.97 levels, you would have to have fuel damage, steam generator tube failures and failure of the diversion to containment feature, which are highly improbable. Main steam radiation monitors are capable of detecting activity that would escape from condenser air ejectors. It is Entergy's position that the existing monitor is adequate to monitor the release point.

**NOTE OO**: The monitor is located and provides radiation level in an area that is not considered part of the plant proper. No radioactivity materials are expected to be brought into this area that would warrant any increase in the range of the existing monitors or the addition of flow monitoring devices.

**NOTE PP***: As per Regulatory Guide 1.97 Rev. 3, seismic qualification is not required for Category II variables. [GENERAL NOTE]

**NOTE QQ**: DELETED

**NOTE RR**: No longer required as per Rev. 3 of Regulatory Guide 1.97.

**NOTE SS**: If the plant vent sampling capability, the wide-range vent monitor, or the main steam line radiation monitor is inoperable in MODES 1, 2, or 3, initiate a preplanned alternate sampling / monitoring capability as soon as practical, but no later than 72 hours after identification of the failure.

**NOTE TT:** The present list of qualified Core Exit Thermocouples is:
K-11, L-12, K-13, C-12, F-12, E-10, D-9, A-11, B-3, B-6, E-5, F-5, G-4, R-10, P-13, H-5, K-3, J-7, N-2, & L-1



336

## 7.6 IN-CORE INSTRUMENTATION

### 7.6.1 Design Basis

The in-core instrumentation is designed to yield information on the neutron flux distribution and fuel assembly outlet temperatures at selected core locations. Using the information obtained from the in-core instrumentation system, it is possible to confirm the reactor core design parameters and calculated hot channel factors. The system provides means for acquiring data and performs no operational plant control.

### 7.6.2 System Design

The in-core instrumentation system consists of thermocouples, positioned to measure fuel assembly coolant outlet temperature at preselected locations; and flux thimbles, which run the length of selected fuel assemblies to measure the neutron flux distribution within the reactor core.

The data obtained from the in-core temperature and flux distribution instrumentation system, in conjunction with previously determined analytical information, can be used to determine the fission power distribution in the core at any time throughout core life. This method is more accurate than using calculational techniques alone. Once the fission power distribution has been established, the thermal power distribution and the thermal and hydraulic limitations determine the core capability and maximum power output.

The in-core instrumentation provides information which may be used to calculate the coolant enthalpy distribution, the fuel burnup distribution, and an estimate of the coolant flow distribution.

Both radial and azimuthal symmetry of power may be evaluated by comparing the detector information from quadrant to quadrant.

#### Thermocouples

Chromel-alumel thermocouples are passed through into guide tubes that penetrate the reactor vessel head through seal assemblies, and terminate at the exit flow end of the fuel assemblies. The thermocouples are provided with two primary seals, a conoseal and swage type seal from conduit to head. The thermocouples are enclosed in stainless steel sheaths within the above tubes to allow replacement if necessary. Thermocouple readings are obtainable via the plant computer and at a manually selected display unit in the control room. The support of the thermocouple guide tubes in the upper core support assembly is described in Chapter 3.

#### Moveable Miniature Neutron Flux Detectors

##### Mechanical Configuration

Six fission chamber detectors (employing $U_3O_8$, which is 93 percent enriched in $U_{235}$) can be remotely positioned in retractable guide thimbles to provide flux mapping of the core. Maximum chamber dimensions are 0.188-inch in diameter and 2.10 inches in length. The stainless steel detector shell is welded to the leading end of the helical wrap drive cable and the stainless steel sheathed coaxial cable. Each detector is designed to have a minimum thermal neutron sensitivity of $1.5 \times 10^{-17}$ amps/nv and a maximum gamma sensitivity of $3 \times 10^{-14}$ amps/R/hr.

Maximum thermal neutron flux for these detectors is 5 x $10^{13}$ nv. Other miniature detectors, such as gamma ionization chambers and boron-lined neutron detectors, can also be used in the system. The basic system for the insertion of these detectors is shown in Figures 7.6-2 to 7.6-4. Retractable thimbles into which the miniature detectors are driven are pushed into the reactor core through conduits which extend from the bottom of the reactor vessel down through the concrete shield area and then up to a thimble seal zone.

The thimbles will be closed at the leading ends, are dry inside, and serve as the pressure barrier between the reactor water pressure and the atmosphere. Mechanical seals provided on the retractable thimbles and on the conduits are shown on Figure 7.6-4.

During reactor operation, the retractable thimbles are stationary. They are extracted downward from the core during refueling to avoid interference within the core. A space above the seal line is provided for the retraction operation.

The drive system for the insertion of the miniature detectors consists basically of six drive assemblies, six 5-path rotary group selector assemblies and six 10-path rotary selector assemblies, as shown in Figures 7.6-2 and 7.6-3. The drive system pushes hollow helical-wrap drive cables into the core with the miniature detectors attached to the leading ends of the cables and small diameter sheathed coaxial cables threaded through the hollow centers back to the ends of the drive cables. Each drive assembly generally consists of a gear motor which pushes a helical-wrap drive cable and detector through a selective thimble path by means of a special drive box and includes a storage device that accommodates the total drive cable length. Further information on mechanical design and support is described in Chapter 3.

Control and Readout Description

The control and readout system provides means for inserting the miniature neutron detectors into the reactor core and withdrawing the detectors at a selected speed while plotting a level of induced radioactivity versus detector position. The control system consists of two sections, one physically mounted with the drive units, and the other contained in the control room. Limit switches in each path provide feedback of path selection operation. Each gear box drives an encoder for position feedback. One 5-path group selector is provided for each drive unit to route the detector into one of the flux thimble groups. A 10-path rotary transfer assembly is a transfer device that is used to route a detector into any one of up to ten selectable paths. Manually operated isolation valves allow free passage of the detector and drive wire when open, and prevents steam leakage from the core in case of a thimble rupture, when closed. A common path is provided to permit cross calibration of the detectors.

The control room contains the necessary equipment for control, position indication, and flux recording. Panels are provided to indicate the core position of the detectors, and for plotting the flux level versus the detector position. Additional panels are provided for such features as drive motor controls, core path selector switches, plotting and gain controls. A "flux-mapping" consists, briefly, of selecting (by panel switches) flux thimbles in given fuel assemblies at various core quadrant locations. The detectors are driven or inserted to the top of the core and stopped automatically. A x-y plot (position vs. flux level) is initiated with the slow withdrawal of the detectors through the core from top to a point below the bottom. In a similar manner other core locations are selected and plotted.

The system that will be used to monitor the distribution of power in the X-Y plane is described in WCAP-7669, "Topical Report – Nuclear Instrumentation System."

BINDER-6

338

# Program Plan
# For
# Hemyc (1-Hour) and M.T. (3-Hour)
# Fire Protective Wrap Performance Testing

Final

January 16, 2003

## 1 Purpose and Scope

Section 50.48, "Fire Protection," of 10 CFR Part 50 requires that each operating nuclear power plant have a fire protection plan that satisfies General Design Criterion 3 of Appendix A to 10 CFR Part 50. Section 50.48 also requires that all plants with operating licenses issued prior to January 1, 1979, satisfy the requirements Sections of III.G, III.J, and III.O of Appendix R to 10 CFR Part 50. (Post 1979 plants (per 10 CFR Part 50.48) have to comply with the provisions of their licenses.)

Section III.G of Appendix R, which addresses fire protection of safe shutdown capability, requires that fire protection features be provided such that one train of systems necessary to achieve hot shutdown conditions remains free of fire damage. One acceptable means of satisfying this requirement is to separate cables and equipment and associated non-safety circuits of redundant systems necessary to achieve and maintain hot shutdown conditions located in the same fire area by a fire barrier having a 3-hour fire rating (Section III.G.2.a). Another means is to enclose cables and equipment and associated non-safety circuits of one redundant train in a fire barrier having a 1-hour fire rating and install fire detectors and an automatic fire suppression system in the fire area (Section III.G.2.c).

The scope of this document is to describe the overall program for investigating the fire protection rating of Hemyc (1-hour) and M.T. (3-hour) fire wraps. The primary approach will be to perform a series of ASTM E 119 furnace tests on a number of cable raceway types that are wrapped in either the Hemyc (with or without air gaps) or M.T. fire barrier material. The Hemyc wrap tests will be performed for a period of 60-minutes each, followed by a hose stream test and post-test visual inspection of the fire wrap. The M.T. test will be similar with the principal difference being that it will be conducted for a period of 3-hours. A description of these tests and of the overall approach are provided below.

## 2 Objective

The objective of this program is to assess the fire protection rating of Hemyc and M.T. fire protection wraps by subjecting various test specimens (conduit, cable trays, cable drops, condolets (access fittings), junction boxes, and raceway support structure analogues) that are enclosed within the wraps to standard temperature-time conditions as specified in NFPA 251 and ASTM E 119. The types and characteristics of the wraps enclosing the test specimens are intended to simulate as-installed configurations.

A secondary objective of these tests is to assess the ability of Rockbestos Surprenant Firezone R fire rated cables to withstand the ASTM E 119 time-temperature environment.

# 3 Approach

The following sections describe the test specimens and the test conditions to be employed for the performance assessments of the Hemyc and M.T. fire barrier systems.

## 3.1 Test specimens

The principal test specimens will include a variety of cable raceway types covered with either the Hemyc 1-hour fire wrap or M.T. 3-hour wrap. In one test, the test specimens will be wrapped with Hemyc fire barrier material directly (i.e., without air gaps). The test specimens in the second test will be enclosed in Hemyc wrap that is framed with structural supports to provide a 5-cm (2 in.) air gap between the wrap and the raceway. For the third test, the test specimens (conduits, condolets, a cable drop and junction box) will be covered with the M.T. fire barrier wrap and subjected to a 3-hour ASTM E 119 furnace exposure. A conduit and condolet LB (an "L" shaped conduit fitting with the access cover on the back, "B") assembly, direct wrapped in Hemyc fire barrier material and a number of support structure specimens directly wrapped with Hemyc material will also be included in the three-hour test, as will three Rockbestos Surprenant Firezone R cables that will be supported in an unwrapped cable tray.

The types of test specimens and the configurations of the fire barrier material wrapping selected for these tests are based principally on the application usage information provided to the NRC/NRR by industry (Letter: Emerson, NEI, to Frumkin, NRC/NRR, "Promatec Hemyc 1-Hour and MT 3-Hour Fire Barrier Systems," December 28, 2001 and via letter: Marion, NEI, to Hannon, NRC/NRR, "Comments on NRC Hemyc Test Plan," December 6, 2002). The testing of the Hemyc wrapped conduit/box assembly during the three-hour test run is being conducted in order to gain some additional data regarding the Hemyc material's performance beyond the one-hour time-temperature exposure conditions.

The testing of empty raceways is intended to provide bounding qualification of the protective material performance under standard test conditions. For example, items of larger thermal mass should be bounded by these tests. Also, this method is per NRC guidance and represents current staff positions on bounding test approaches. Additionally, it is also intended that the assembly and installation of the Hemyc and M.T. fire barriers will be done in accordance with the vendor's specifications and meet all required vendor quality standards.

The test specimens will include the following items:

- A 27-mm (1 in.) steel conduit arranged in a modified "U" configuration such that one vertical leg and one end of the horizontal span of the conduit intersect at a condolet LB access fitting, forming a right angle, while the other end of the horizontal span transitions to the second vertical leg via a conduit radius bend or elbow.
- A 63-mm (2½ in.) steel conduit arranged in a modified "U" configuration such that one vertical leg and one end of the horizontal span of the conduit intersect at a condolet LB access fitting, forming a right angle, while the other end of the horizontal span will transition to the second vertical leg by means of a conduit radius bend or elbow.
- A 103-mm (4 in.) steel conduit arranged in a modified "U" configuration such that one

vertical leg and one end of the horizontal span of the conduit intersect at a 30 cm x 61 cm x 25 cm (12" x 24" x 10") steel junction box, forming a right angle, while the other end of the horizontal span will transition to the second vertical leg through a conduit radius bend or elbow in one of the one-hour tests. For the three-hour test, the large diameter (103-mm) conduit will be coupled to the junction box at the mid-point of its horizontal span to allow a cable drop to intersect the top of the box from the furnace ceiling. In that test the sharp right angle transition will employ a large condolet LB fitting while the other horizontal-to-vertical transition will be made by means of a radius bend or elbow.

- A 305-mm (12 in.) wide steel ladder-back cable tray. The cable tray will be constructed in a modified "U" configuration such that one vertical leg and one end of the horizontal span of the conduit intersect at a right angle, while the other end of the horizontal span will transition to the second vertical leg by means of a tray vertical curve.
- A 610-mm (24 in.) wide steel ladder-back cable tray. The cable tray will be constructed in a modified "U" configuration such that one vertical leg and one end of the horizontal span of the conduit intersect at a right angle, while the other end of the horizontal span will transition to the second vertical leg by means of a tray vertical curve.
- A 914-mm (36 in.) wide steel ladder-back cable tray. The cable tray will be constructed in a modified "U" configuration such that one vertical leg and one end of the horizontal span of the conduit intersect at a right angle, while the other end of the horizontal span will transition to the second vertical leg by means of a tray vertical curve.
- Two short cable drops: one consisting of a single 8 AWG bare copper wire and the other being a 250 kcmil bare copper wire.
- Four separate support structure test elements consisting of four different cross sections (threaded rod, Unistrut®, angle iron and square tube) formed into a right angle ("L") configuration and partially covered by the Hemyc material. These structures are being included in the test program to evaluate the magnitude of heat transmission along their wrapped length and the possible thermal coupling effect on any supported assemblies.

In addition, three Rockbestos Surprenant Firezone R cables will be subjected to the furnace environment during the three-hour test in order to evaluate their ability to withstand the ASTM E 119 time-temperature profile. One each of a power (3 conductor), control (5 conductor) and instrument (2 conductor) type cables will be tested. These cables will be placed and secured in a separate, unwrapped 305-mm (12 in.) wide ladder-back cable tray during the three-hour test. During the test, the insulation resistance (IR) between the individual conductors to all of the other conductors in the Firezone R cables, and the IR between the individual conductors and electrical ground will be monitored continuously during the test using the Sandia Insulation Resistance Measurement System. The 305-mm steel cable tray supporting the three Firezone R cables will be electrically isolated from the other raceway test specimens.

Each of the fire protection wrapped cable raceway test specimens will be tested without any cables routed through them. A bare #8 copper conductor, instrumented with thermocouples along its length, will be routed through each of the raceway test specimens. The thermocouples will be attached to the bare copper conductor at 150-mm (6 in.) spacing

intervals. Additional thermocouples will be attached to the outer surfaces of the conduit test specimens and along the length of both side rails of the cable tray test specimens at 150-mm intervals. The protective wrap at one end of each conduit test specimen will be flared and attached to the furnace ceiling interface. The opposite end of these conduit test specimens will be insulated with fiber filler inside and around the outside wall at the ceiling interface. Likewise, the protective wrap at the top of all cable drops will be flared around the furnace ceiling penetration while the cable drop interface with other test specimens (tray or junction box) will not be flared.

Table 1 presents the test conditions to be investigated in terms of fire wrap type and configuration of each of the test specimens during each test. Note that no conduits will be tested in the air gap framed configuration and that no trays will be tested with M.T. wrap. Also, the support structure specimens will be protected only with direct wrap Hemyc material in the tests using both 38-mm (1½ in.) and 50-mm (2 in.) thicknesses. In addition, a 27-mm (1 in.) conduit and condolet LB assembly, wrapped with Hemyc fire wrap will be included in the three-hour test.

**Table 1. Test Matrix**

| | Test 1 | Test 2 | Test 3 |
|---|---|---|---|
| | Hemyc (1-Hour Direct Wrap) | Hemyc (Framed for Air Gap) | M.T. (3-Hour Direct Wrap) |
| 27-mm Conduit | X | (Not included) | X* |
| 63-mm Conduit | X | (Not included) | X |
| 103-mm Conduit | X | (Not included) | X |
| 305- mm Tray | X | X | (Not included) |
| 610-mm Tray | X | X | (Not included) |
| 914-mm Tray | X | X | (Not included) |
| 8 AWG Cable Drop | X | X | X |
| 250 kcmil Cable Drop | X | X | (Not included) |
| Junction Box | X | X | X |
| Support Structures | X | (Hemyc direct wrap) | (Hemyc direct wrap) |
| Firezone R Cables | (Not included) | (Not included) | (No protective wrap) |

* Test 3 will also include a separate 27-mm conduit test specimen direct wrapped in Hemyc material.

A detailed construction plan for each of the test specimens will be developed. The plan will

define the specific details of the design and assembly of each test specimen and the installation of the designated fire wrap. Drawings and descriptions of the dimensions and setup configurations in the furnace and instrumentation details will also be provided. The fabrication and installation of the fire protective wraps will conducted be in accordance with vendor procedures and provisions will be made to verify that all material/installation quality requirements are met. The detailed construction plan is expected to be distributed as an appendix to the final test plan.

Following the completion of the detailed construction plan and final test plan the required materials and equipment will be procured. The type of material and equipment obtained will include cables, raceways (conduit, trays, condolets, and junction boxes), metal to fabricate the support structure specimens, Hemyc and M.T. fire barrier wrap assemblies, framing material for the fire barrier wraps, thermocouples and extension wire, miscellaneous hardware (nuts, bolts, screws, etc.) plus spare parts.

The test specimens will be assembled in accordance with the detailed construction plan as the material and equipment are obtained. The process will include the installation of the thermocouples to the outer surfaces of the test specimens and checkout for proper operation prior to the installation of the fire barrier wraps. It is possible that assembly checklists will be developed for each of the test specimens and included as part of the final test plan. The fire barrier wraps will be installed around the test specimens per the manufacturer's procedures.

Photographs of the test specimens, both during and after assembly, will be taken prior to testing and kept as part of the test documentation.

### 3.2 Test criteria

The test specimens will be subjected to the ASTM E 119 time-temperature profile in the test furnace. An assessment of the fire barrier wrap performance will be based on two principal factors:

1. *The time at which the average unexposed side temperature of the fire barrier system, as measured on the exterior surface of the raceway or component, exceeds 139 C (250 F) above its initial temperature. Or the time at which a single temperature reading of a test specimen exceeds 30% of the maximum allowable temperature rise (i.e., 181 C [325 F]) above its initial temperature.*

2. *The fire barrier system remains intact during the fire exposure and water hose stream test without developing any openings through which the cable raceway is visible.*

### 3.3 Test facilities

A Request for Proposal will be distributed soliciting bids on providing test services for the primary test series. Included in the RFP will be a discussion of the scope of the tests, specific

tasks to be performed, and furnace requirements. Desirable facility support capabilities will include the availability of a test specimen assembly area, data acquisition interfaces for the test specimen thermocouples, providing photo/video records of the test specimens and tests, and a summary report/documentation of the conduct of each test.

Upon receipt of the proposals, they will be evaluated against the predetermined selection criteria until two finalists are left. It is expected that site visits will be made by SNL and/or NRC representatives to evaluate the specific capabilities and furnace dimensions to be incorporated into the detailed construction plan. Based on the results of these visits a finalist will be chosen and a contract will be negotiated and placed.

## 3.4 Primary tests

Three separate test runs will be conducted as part of the primary test series. Two of the tests will test the performance of 1-hour Hemyc fire barrier wrap systems and the third test will assess the performance of 3-hour M.T. fire barrier wrap. All of the primary tests will be conducted using the ASTM E 119 standard time-temperature furnace profile (Figure 1).

As indicated above, these tests will be governed by the conditions provided in a formal test plan. Initially, a draft test plan will be written for review and comment by NRC. Then the final test plan, incorporating the changes directed by NRC, will be issued.

The test specimens will consist of those items described in Section 3.1, Test Specimens, above. The specific setup and configuration for each test is discussed below. It should be noted, however, that the test conditions and configurations described below assume the availability and use of a floor furnace of specific dimensions; based on the outcome of the testing services solicitation and contracting process, certain details may require modification.

### 3.4.1 Test #1

The first test of the primary test series will be conducted on eleven test specimens directly wrapped with Hemyc fire barrier blankets (i.e., without framework to provide air gaps between the wrap and raceways). The nominal thickness of the protective blankets will be 38 mm (1½ in.) for the cable trays and 50 mm (2 in.) for the conduit and cable drops. One of the support structure specimens will be wrapped with a 38 mm thick Hemyc blanket and the other with a 50 mm thick blanket.

Figure 2 shows the planned configuration of the test specimens inside the furnace. Looking at the elevation and plan views in the figure, the arrangement of the test specimens is as follows (from left to right):

- The 27-mm (1 in.) conduit and condolet LB assembly,
- the 305-mm (12 in.) wide cable tray with the small (8 AWG) cable drop entering from above,
- two support structures (both formed out of threaded rod),
- the 610-mm (24 in.) wide cable tray with the large (250 kcmil) cable drop entering from above,

- the 103-mm (4 in.) conduit and 30 cm X 61 cm X 25 cm (12" x 24" x 10") junction box assembly,
- the 914-mm (36 in.) cable tray, and
- the 63-mm (2½ in.) conduit and condolet LB assembly.

This arrangement of the test specimens was selected in order to minimize the potential for one specimen to influence the response of another specimen to the thermal environment. Note that one end of each conduit test specimen has its protective wrap flared around the furnace ceiling penetration.

The conduit and cable trays will be supported from the furnace ceiling in a modified "U" configuration. Each tray and conduit will include one sharp 90-degree transition from the horizontal span to one of the vertical legs. At the other transition point a radius bend will be used. In the case of the conduit test specimens, a condolet fitting or junction box will be employed to provide the right angle transition from horizontal to vertical. The cable trays will be modified and assembled to accommodate the right angle turn. The two vertical runs of these test articles will be approximately 0.6 m (24 in.) along each leg and the horizontal span will be ~1.4 m (54 in.).

Other test specimens will include two cable drop bundles and support structure analogues. A direct wrap cable bundle (250 kcmil bare copper wire) will be dropped through the top of the furnace and join the 610-mm (24 in.) cable tray at its mid-point. Sirnilarly, a smaller (8 AWG bare copper wire) direct wrapped cable bundle will be dropped through the top of the furnace and join the 305-mm (12 in.) cable tray at its mid-point. The two partially direct wrapped support structure test specimens will be hung from the top of the furnace. The temperature data collected from these articles will be used to evaluate the potential transmission of heat along the wrapped portion of the specimens.

The minimum distance from the furnace walls and the test specimens will be 30 cm (12 in.) and the minimum distance between adjacent test specimens will be ~33 cm (13 in.).

### 3.4.2 Test #2

The second primary test will be conducted on twelve test specimens, six of which will be wrapped with Hemyc fire barrier blankets and employing the necessary framework to provide a minimum of 50-mm (2 in.) air gaps between the wrap and item. The nominal thickness of the protective blankets will be 38 mm (1½ in.). This test will also include six support structure test specimens, directly wrapped in the Hemyc fire barrier material without employing the 50-mm air gap. Three of the support structure specimens–one of each cross section–will be covered with a 38-mm (1½ in.) thick Hemyc wrap and the remaining three will be covered with a 50-mm (2 in.) thick wrap.

The planned arrangement of the test specimens in the furnace during Test #2 is shown in Figure 3. Looking at the elevation and plan views in the figure, the arrangement of the test specimens is as follows (from left to right):

- The 305-mm (12 in.) wide cable tray with the small (8 AWG) cable drop bundle entering from above,

- two support structures made of tube steel with 75 mm x 75 mm square cross sections,
- the 610-mm (24 in.) wide cable tray with the large (250 kcmil) cable bundle entering from above,
- two support structures made of Unistrut®,
- the 30 cm x 61 cm x 25 cm (12" x 24" x 10") junction box,
- two support structures made of angle iron, and
- the 914-mm (36 in.) cable tray.

This arrangement of the test specimens was selected in order to minimize the potential for one specimen to influence the response of another specimen to the thermal environment.

As was the case for Test #1, the cable trays will be supported from the furnace ceiling in a modified "U" configuration. Each tray and conduit will include one sharp 90-degree transition from the horizontal span to one of the vertical legs. At the other transition a radius bend will be used. The cable trays will be modified and assembled to accommodate the right angle turn. The two vertical runs of these test articles will be approximately 0.6 m (24 in.) along each leg and the horizontal span will be ~1.3 m (50 in.).

The junction box will be supported from the furnace ceiling by two Unistrut® channels that are hung on four threaded rods. These junction box supports will be directly wrapped with Hemyc material separately from the box. (Note that the junction box supports are not considered as part of this test and will not be instrumented; however any failure in their performance during the test will be noted and investigated as deemed appropriate.) A wrapped (250 kcmil bare copper wire, with air gap) cable bundle will be dropped through the top of the furnace and join the 610-mm (24 in.) cable tray at its mid-point. Another wrapped cable bundle (8 AWG bare copper wire, with air gap) will be dropped through the top of the furnace and join the 305-mm (12 in.) cable tray at it mid-point. The partially direct wrapped support structure test specimens will be hung from the top of the furnace. The temperature data collected from these articles will be used to evaluate the potential transmission of heat along the wrapped portion of the specimens.

The minimum distance from the furnace walls and the test specimens will be 30 cm (12 in.) and the minimum distance between adjacent test specimens will be ~25 cm (10 in.).

### 3.4.3 Test #3

The final test of the primary test series will be conducted on eleven test specimens, five of which will be wrapped with M.T. 3-hour fire barrier blankets but without any framework to provide air gaps between the wrap and raceway. The nominal thickness of the M.T. protective covering will be ~76 mm (3 in.). In addition, four structural support specimens, partially wrapped in 38-mm (1½ in.) thick Hemyc wrap (direct wrapped), and one 27-mm (1 in.) conduit/pull box enclosed in Hemyc wrap, also direct wrapped, will be included in the third test.

Three Rockbestos Surprenant Firezone R cables will be supported in an unwrapped 305-mm (12 in.) wide steel ladder back cable tray inside the furnace for this test. These cables will be continuously monitored for changes in their insulation resistance (conductor-to-conductor and

conductor-to-ground) during the three hour long test.

Figure 4 shows the configuration of the test specimens in the furnace during Test 3. Looking at the elevation and plan views in the figure, the arrangement of the test specimens is as follows (from left to right):

- The 27-mm (1 in.) conduit and condolet LB assembly, wrapped in M.T. material;
- two support structures (one 75 mm x 75 mm square cross section tube steel and one angle iron), directly wrapped in Hemyc material;
- the 103-mm (4 in.) conduit and 30 cm x 61 cm x 25 cm (12" x 24" x 10") junction box assembly, wrapped in M.T. material with a small cable bundle, also wrapped with M.T., entering at the top of the junction box;
- two support structures ( one Unistrut® channel and one threaded rod), directly wrapped with Hemyc material;
- the 63-mm (2½ in.) conduit and pull box assembly, wrapped in M.T. material;
- one 27-mm (1 in.) conduit and pull box, directly wrapped in Hemyc material; and
- the unprotected 305-mm (12 in.) cable tray containing the three Firezone R test cables.

As in the other two tests, the conduit assemblies will be supported from the furnace ceiling in a modified "U" configuration. Each conduit will include one sharp 90-degree transition from the horizontal span to one of the vertical legs and a radius bend will be used for the other transition. A condolet fitting will be employed to provide the right angle turn. The two vertical runs of these test articles will be approximately 0.6 m (24 in.) along each leg and the horizontal run will be ~1.3 m (50 in.). One end of each conduit assembly will have its protective wrap flared at the furnace ceiling interface.

No cable trays are included as test specimens for this test. The four partially protected (direct Hemyc wrap only–no air gap) support structure test specimens will be hung from the top of the furnace in between the other test specimen groups.

The unwrapped 305-mm (12 in.) cable tray will be supported from the furnace ceiling in a "U" configuration. This tray is being employed only to support the fire resistant Rockbestos cables, thus the tray will not include any sharp horizontal-to-vertical transitions. The purpose for including these Firezone R cables in the test is to determine their ability to withstand the ASTM E 119 temperature conditions.

The minimum distance from the furnace walls and the test specimens will be 30 cm (12 in.) and the minimum distance between adjacent test specimens will be 45 cm (18 in.).

### 3.5 Conduct of tests

Each of the primary test runs will be conducted by exposing the test specimens to the time-temperature profile as specified in ASTM E 119, Standard Test Methods for Fire Tests of Building Construction and Materials. By this method, the temperature inside the furnace should reach 927 C (1700 F) at the end of the one-hour tests and 1052 C (1925 F) at the end of the 3-hour test. Figure 1 shows the desired temperature profile as a function of time.

The insulation resistance of the three Rockbestos Surprenant Firezone R cables will be monitored continuously during the three-hour test. The insulation resistance of each conductor in the test cable to the other conductors in the cables as well as the insulation resistance between each conductor in the test cables to ground will be recorded as a function of time using the Sandia Insulation Resistance Measurement System. A single-phase 120 VAC source will be applied to each conductor in turn while leakage currents generated in the other conductors is monitored and logged. Peak leakage currents will be limited to 1 A or less. The cable tray supporting the Firezone R cables will be connected to electrical ground.

Upon completion of each ASTM E 119 temperature run (one- and three-hours), the furnace will be opened (or the complete test assembly will be removed from the furnace) and a hose stream will be applied to all of the test articles. The hose stream test will consist of a water stream applied at random to all exposed surfaces of the test specimens through a 38-mm (1½ in.) fog nozzle set at a discharge angle of 15 degrees with a nozzle pressure of 517 kPa (75 psi) at a minimum discharge rate of 284 lpm (75 gpm) with the tip of the nozzle at a maximum distance of 3 m (10 ft) from the test specimen. The hose stream application will be continued for at least 5 minutes upon completion of the test.

A visual inspection of all test articles will be conducted following the hose stream test. The purpose of the inspection will be to ascertain whether the fire barrier wraps remained intact during the fire exposure and hose stream test without developing any openings or breaches. Visible indications of an opening will include obvious tears or displacement of a wrap section or a view of the covered raceway through the wrap.

Photographs of the test specimens, both prior to and after disassembly, will be taken during the post-test inspection and kept as part of the test documentation.

### 3.6 Instrumentation and data collection

The primary data to be generated in these tests will be component temperatures as indicated by Type-K thermocouples. Test #1 will require the use of ~340 thermocouples and Test #2 will require ~240 thermocouples. Approximately 270 thermocouples will be needed for Test #3. The outputs of the thermocouples will be sent to a computerized data collection unit for recording and storage. Each thermocouple's output will be recorded at least once per minute. It is expected that Teflon coated thermocouples will be used during the M.T. test (Test #3) to ensure that there will not be interference from any gases evolving from the protective wraps.

Figures 5-12 show the preferred attachment locations of the thermocouples on the conduit, trays, cable drops, junction box and support structure test specimens during the three tests. Routing the thermocouples for monitoring the tray temperatures will be by laying the bundles in the tray at the entry point and branching the thermocouples off for attachment to the tray rails and bare copper conductor at the appropriate locations. Similarly, for the cable drop thermocouples, the thermocouples will be bundled with the cable drop cables at the point of entrance on the ceiling of the furnace and branching off the thermocouples for attachment to the bare copper conductor wire at the appropriate points.

Each conduit will have thermocouples attached to the outer surface located along the outside

perimeter of the "U" shape (see Figures 5, 7 , 9 and 12). The routing of thermocouples for monitoring the temperature of the conduit will require that a series of small thermocouple bundles be placed around the circumference of the conduit and run to their individual attachment locations between the conduit and fire wrap. In order to minimize the effect of these small bundles on the test results, the conduit thermocouples will be run in underneath the wrap from both ends of the test specimen. In addition, the bare copper wires routed through the interior of the conduit test specimens will also be instrumented with thermocouples. The junction boxes and condolet fittings will have at least one thermocouple attached to each side (6 in all) located at or as closely as possible to the geometric center of the side walls.

The reader should note that the thermocouple locations indicated in these figures are for information purposes only. The thermocouples will be installed at 150-mm (6 in.) intervals along the conduits, cable tray rails, condolets, junction boxes, and bare #8 copper wires in accordance with the guidance provided in Supplement 1 to Generic Letter (GL) 86-10 and Regulatory Guide (RG) 1.189.

The Sandia Insulation Resistance Measurement System will be used to monitor the changes in insulation resistance occurring within the Rockbestos Surprenant Firezone R cables during Test 3. The concept of the SNL IR measurement system is based on the assumption that if one were to impress a unique signature voltage on each conductor in a cable (or cable bundle), then by systematically allowing for and monitoring known current leakage paths, it should be possible to determine if leakage from one conductor to another, or to ground, is in fact occurring. That is, part or the entire voltage signature may be detected on any of the other conductors in the cable (or in an adjacent cable), or may leak to ground directly.

To illustrate, consider a three-conductor (3/C) cable, as illustrated in Figure 13. If 100 V are applied to Conductor 2, the degree of isolation of Conductors 1and 3 from Conductor 2 can be determined by systematically opening a potential conductor-to-conductor current leakage path and then reading the voltages of each conductor in turn while Conductor 2 is energized. Determining the IR between Conductors 1 and 2 at the time of voltage measurement on Conductor 2 is a simple calculation employing Ohm's law.

The calculation of the three resistances for each conductor pair (one conductor-to-conductor path and each of the two conductor-to-ground paths) requires the measured voltages ($V_i$ and $V_j$) for two complementary switching configurations. For example, the complement for the case illustrated in Figure 13 is shown in Figure 14. As illustrated in Figure 13, Conductor 2 is connected to the input side and conductor 3 is connected to the measurement side. The complementary case shows Conductor 3 on the input side and Conductor 2 on the measurement side, as shown in Figure 14. This complementary pair provides four separate voltage readings that can be used to determine the three resistance paths affecting these two conductors; namely, $R_{2\text{-}3}$, $R_{2\text{-}G}$, and $R_{3\text{-}G}$.

This concept is scalable for virtually any number of conductors in a cable or bundle of cables. Another advantage is that only the two voltage measurements for each switching configuration need to be recorded in real time; determining the resistances can be deferred until after the test is completed.

Employing this method to monitor the changes in insulation resistance of the individual conductors in the Firezone R cables during the furnace test will provide sufficient data to determine the degree, if any, of cable degradation. In addition, this method is able to identify the indications of insulation resistance recovery (e.g., healing) as the temperature of the furnace is decreased following the test period. Since the Sandia IR measurement system presently exists and has been demonstrated previously the cost impact to the program to include the Firezone R cables' IR measurements is expected to be small.

### 3.7 Follow-on tests

The decision to plan and conduct follow-on tests will be made on the basis of the primary test results.

## 4 Reporting and Documentation

The test data will be analyzed and the fire barrier performance will be evaluated based on the acceptance criteria. A test report will be submitted to NRC that will include recommendations, if any, for follow-on testing.

It should be recognized that the possibility exists that these test results may form the technical basis for broad acceptance of these fire protection systems by NRC, or provided the basis for enforcement action or backfit requirements, as deemed appropriate.

## 5 Recommendation for Research Enhancements

The appendix to this document proposes several modifications to this plan that would enhance the quality of these tests for research purposes. These suggestions are based in large measure on comments received from industry (letter: Marion, NEI, to Hannon, NRC/NRR, "Comments on NRC Hemyc Test Plan," December 6, 2002) on the previous draft of this program plan.

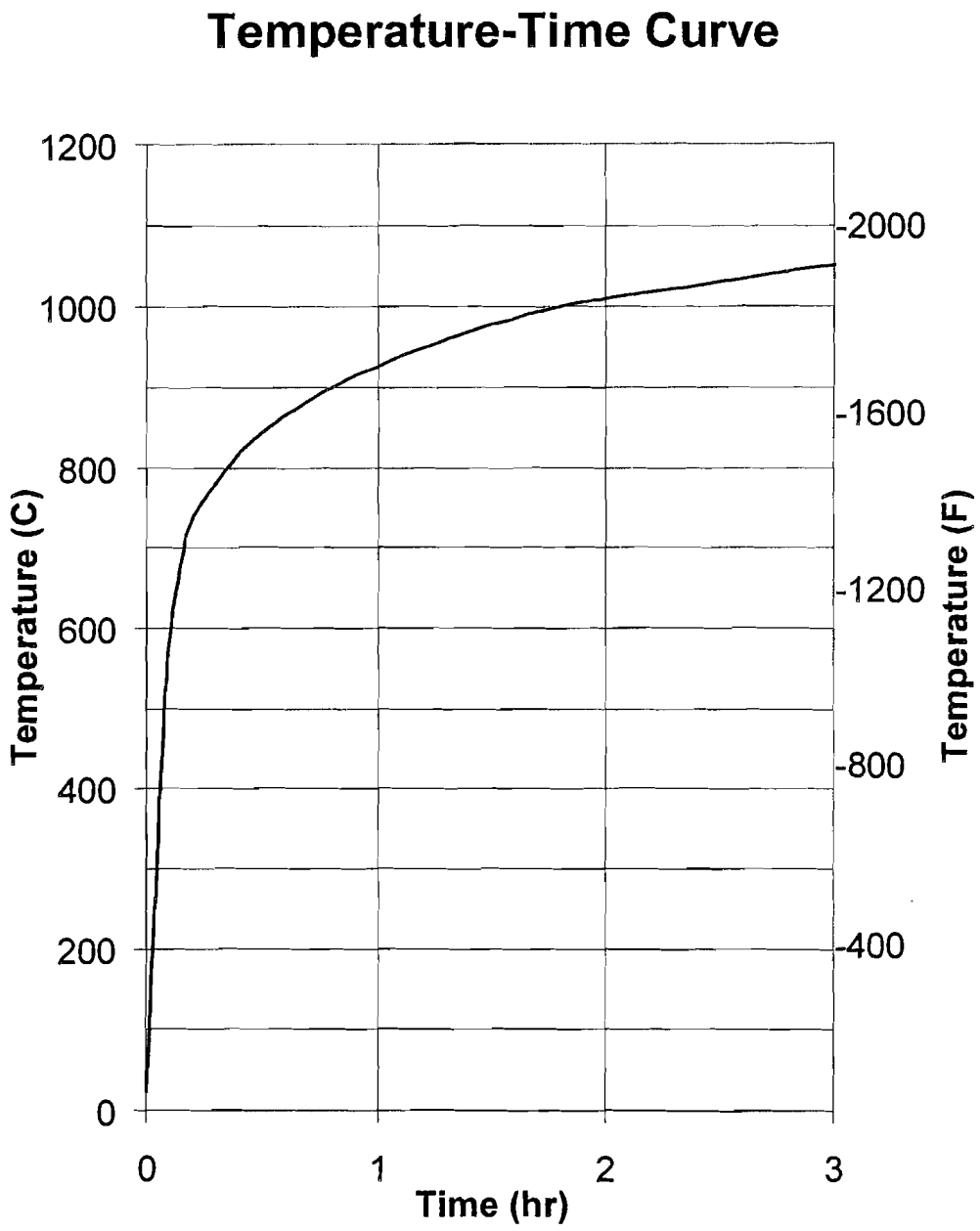


**Figure 1:** Excerpt of the Standard Time-Temperature Curve (based on data provided in ASTM E 119).

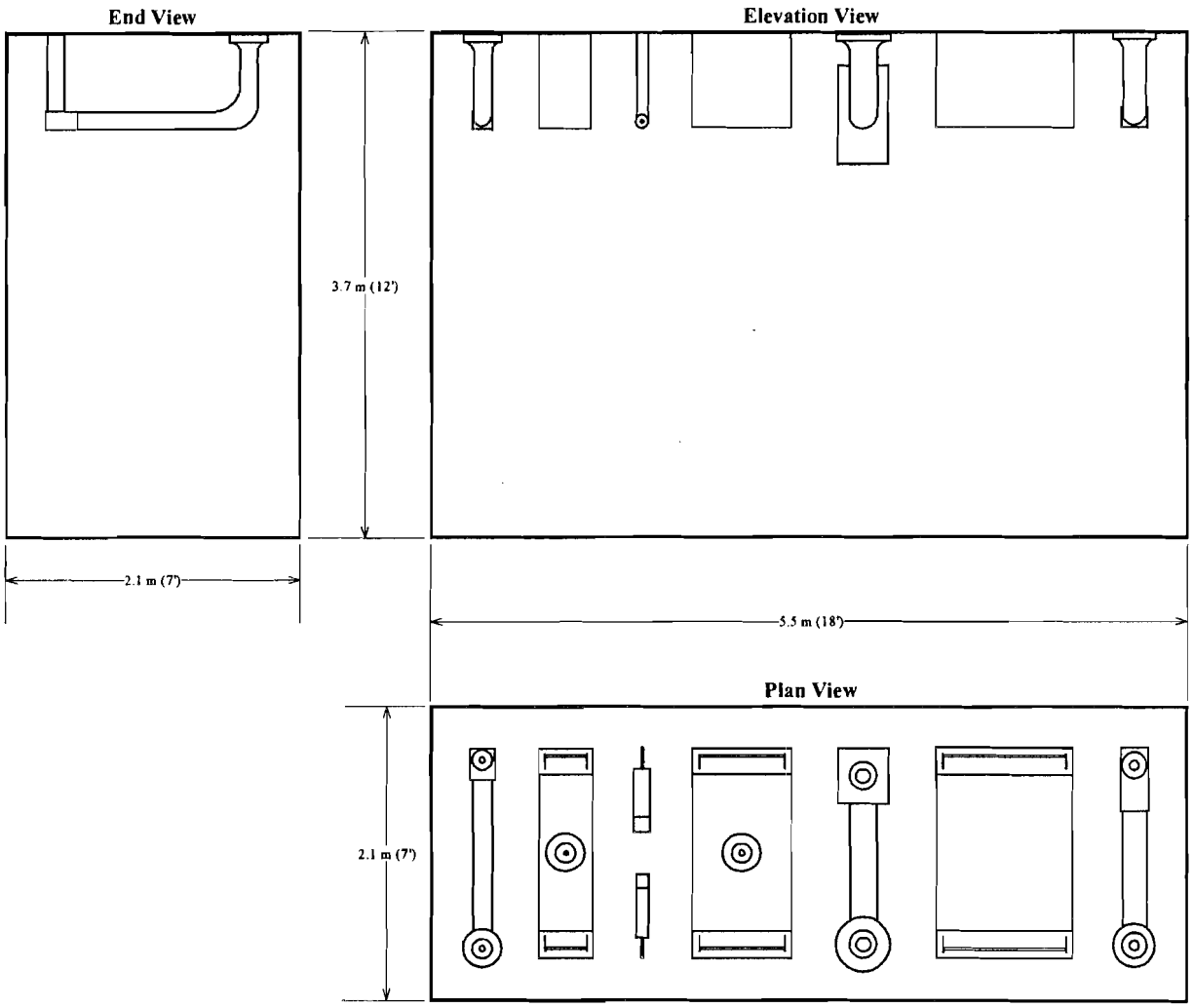


**Figure 2:** Test Specimen Layout for Test 1.

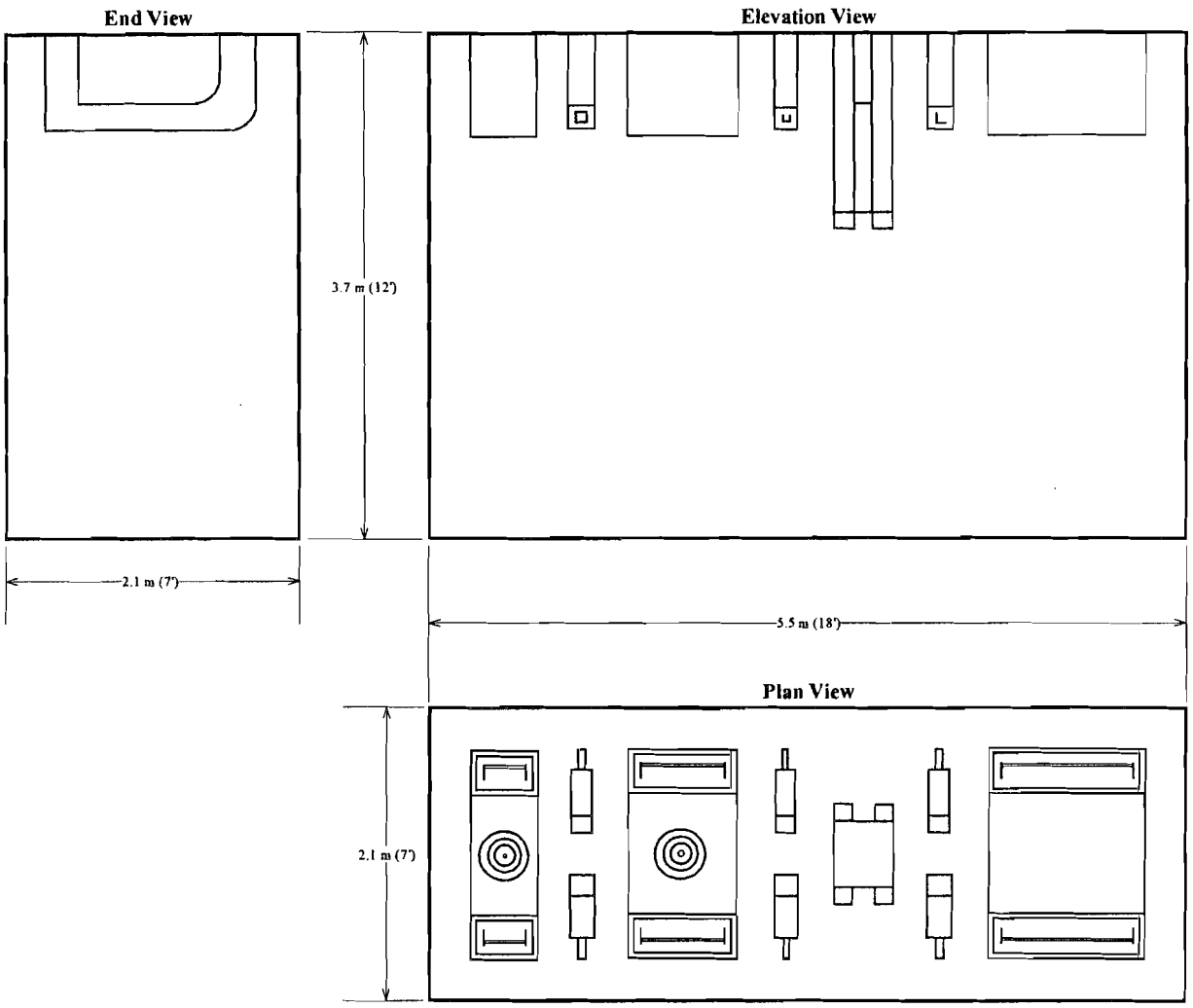


**Figure 3:** Test Specimen Layout for Test 2.

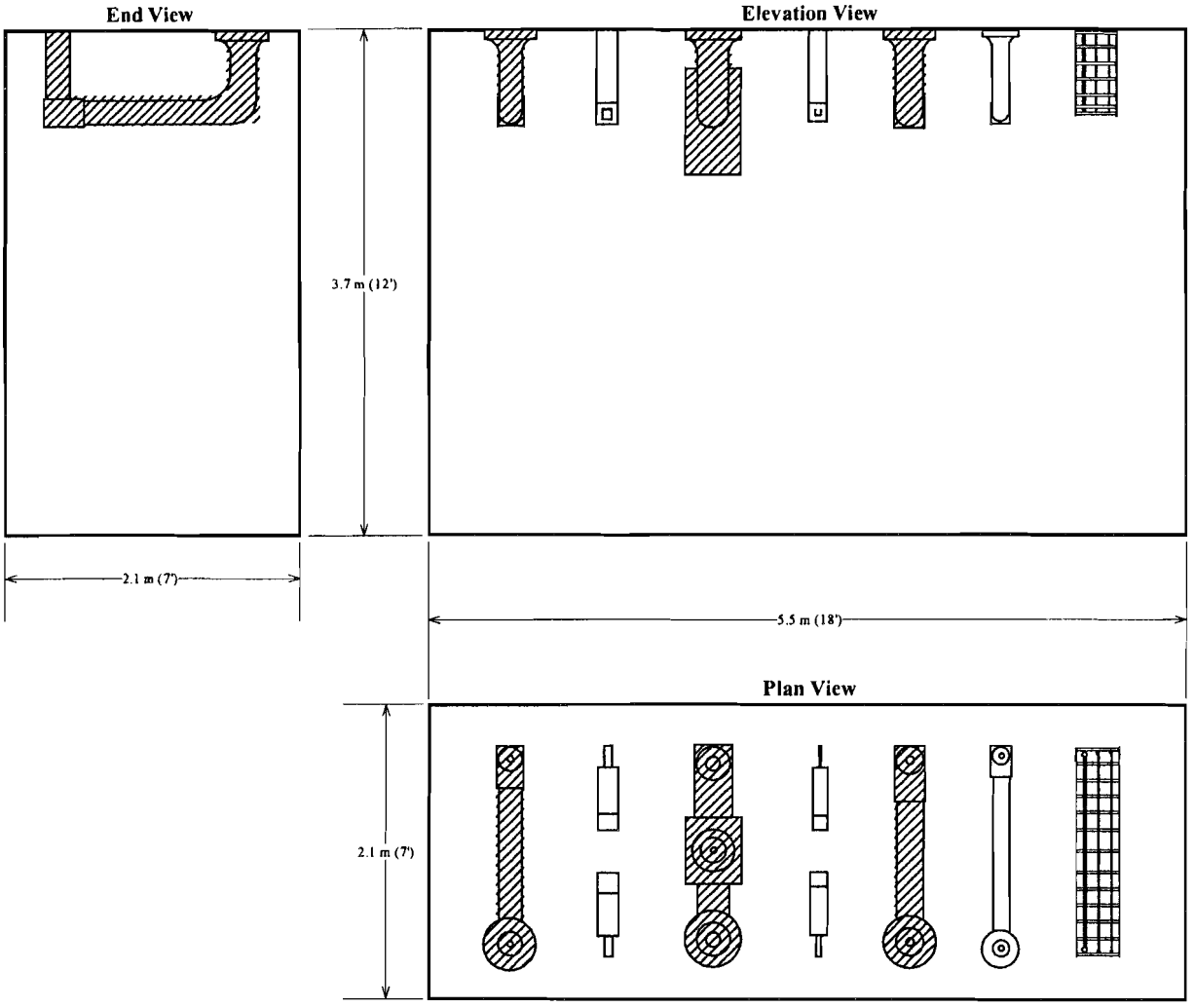


**Figure 4:** Test Specimen Layout for Test 3. Note that the shaded elements represent the test specimens protected with the M.T. fire wrap. Unshaded elements are enclosed in Hemyc fire wrap. The Firezone R fire rated cables will be installed in an unprotected, open cable tray.

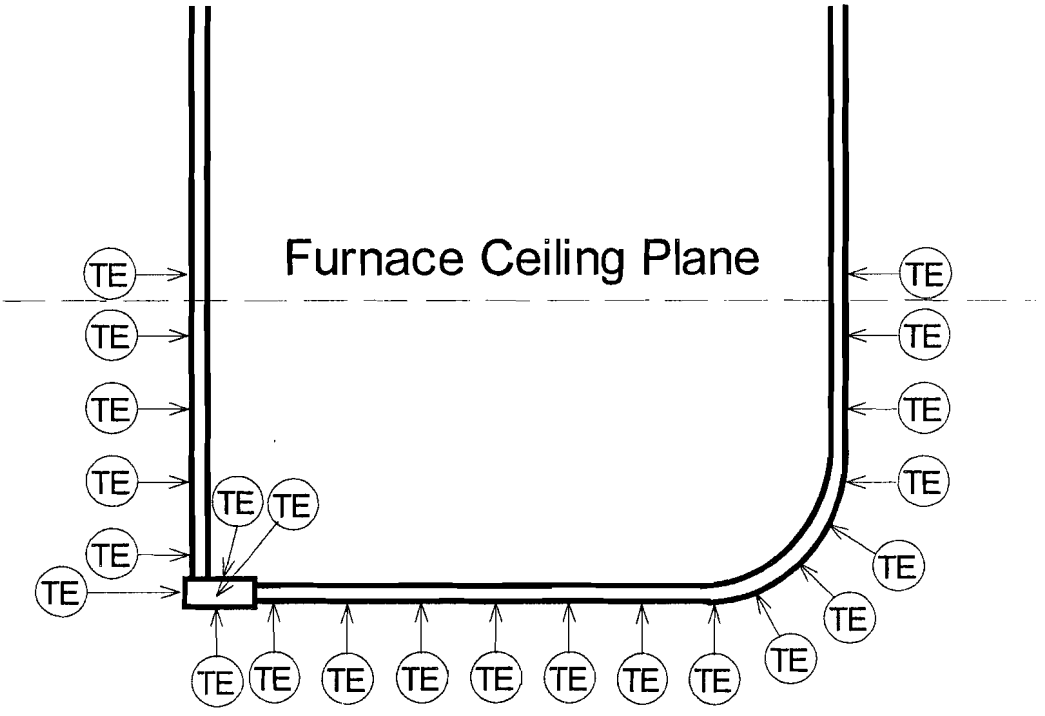


**Figure 5:** Planned Thermocouple Locations on 27-mm (1 in.) Conduit/Condolet LB Test Specimens. Note that at least one thermocouple will be attached to each face of the condolet fitting. A single bare copper wire (8 AWG) will be instrumented with thermocouples and routed inside the test specimen.

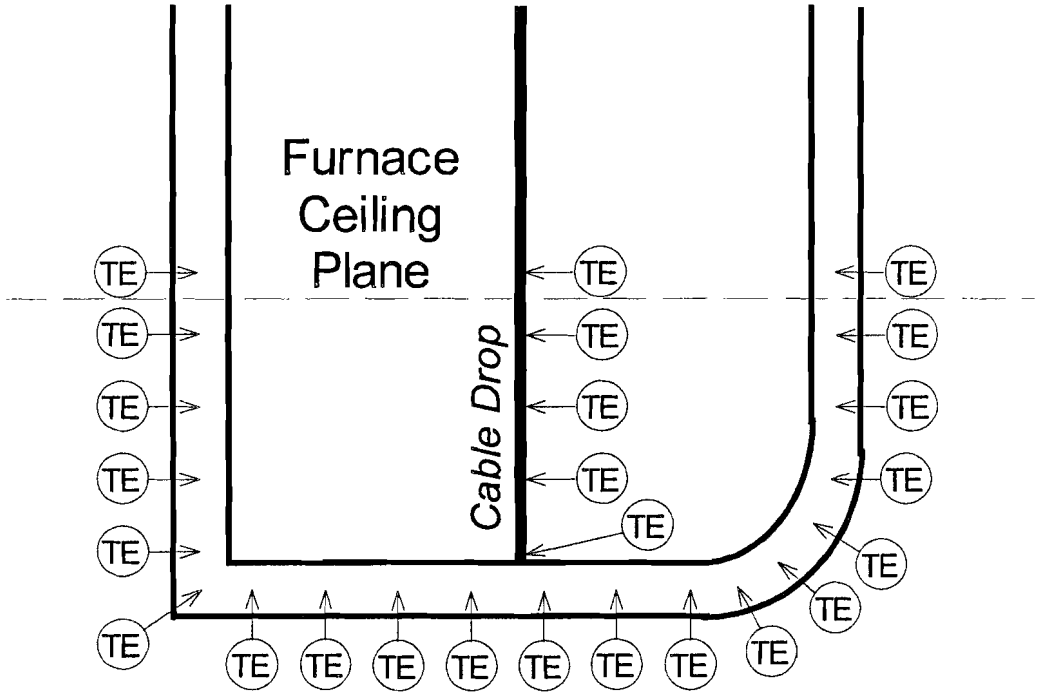


**Figure 6:** Planned Thermocouple Locations on the 305-mm (12 in.) and 610-mm (24 in.) Cable Tray Test Specimens during Tests #1 and #2. Note that the locations indicated reflect relative positions on each tray side rail and on the bare 8 AWG copper wire attached to the tray rungs. Also, note that the cable drop will consist of a bare 250 kcmil (610-mm tray) or a 8 AWG (305-mm tray) copper wire to which the thermocouples are attached.

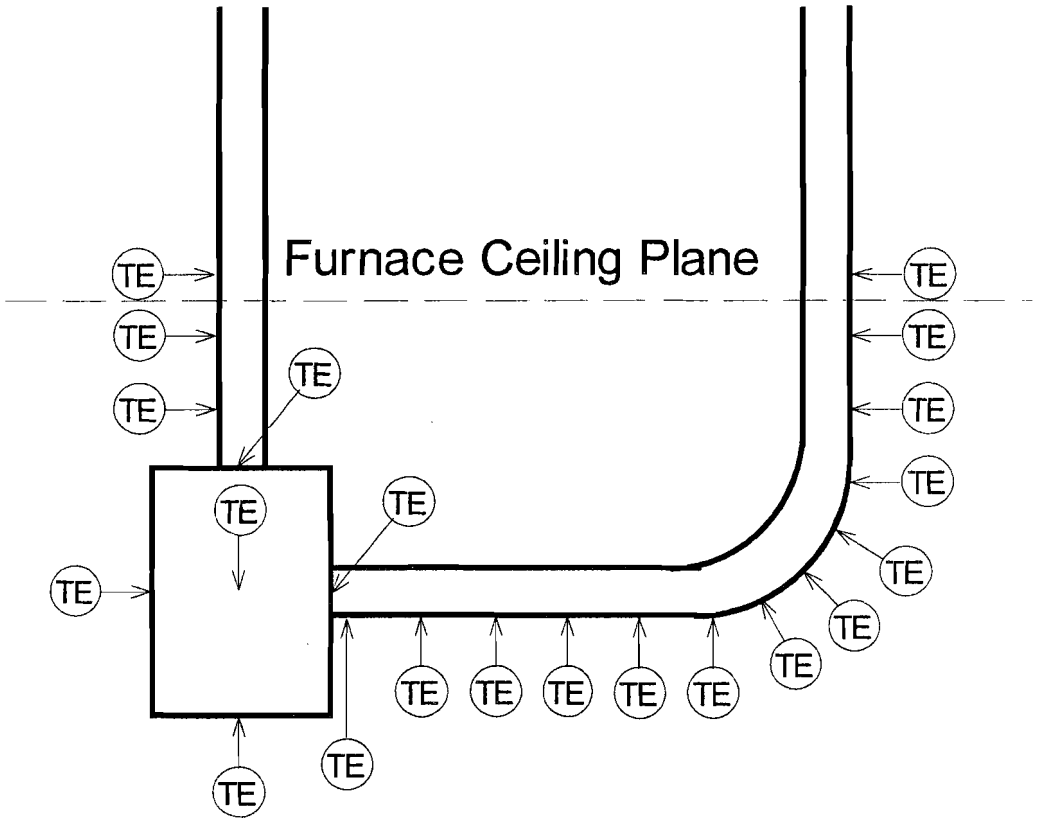


**Figure 7:** Planned Thermocouple Locations on the 103-mm (4 in.) Conduit and Junction Box Assemblies during Test #1. Note that a thermocouple will be attached to each face of the junction box (6 total). A single bare copper wire (8 AWG) will be instrumented with thermocouples and routed inside the test specimen.

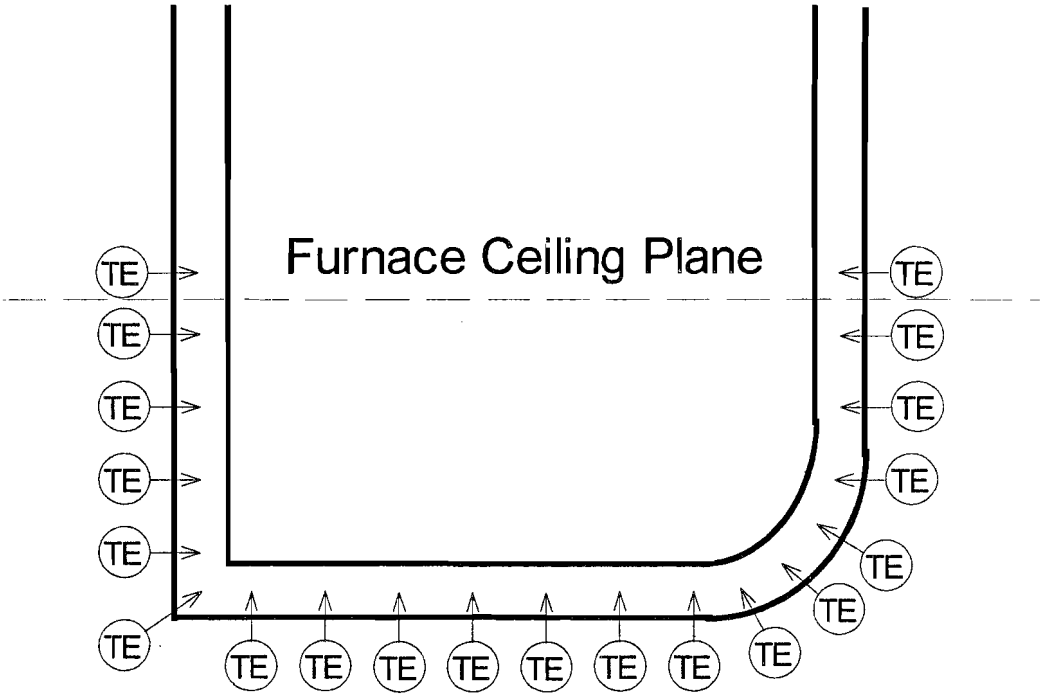


**Figure 8:** Planned Thermocouple Locations on the 914-mm (36 in.) Cable Tray Test Specimens. Note that the locations indicated reflect relative positions on each tray side rail and on the bare 8 AWG copper wire attached to the tray rungs.

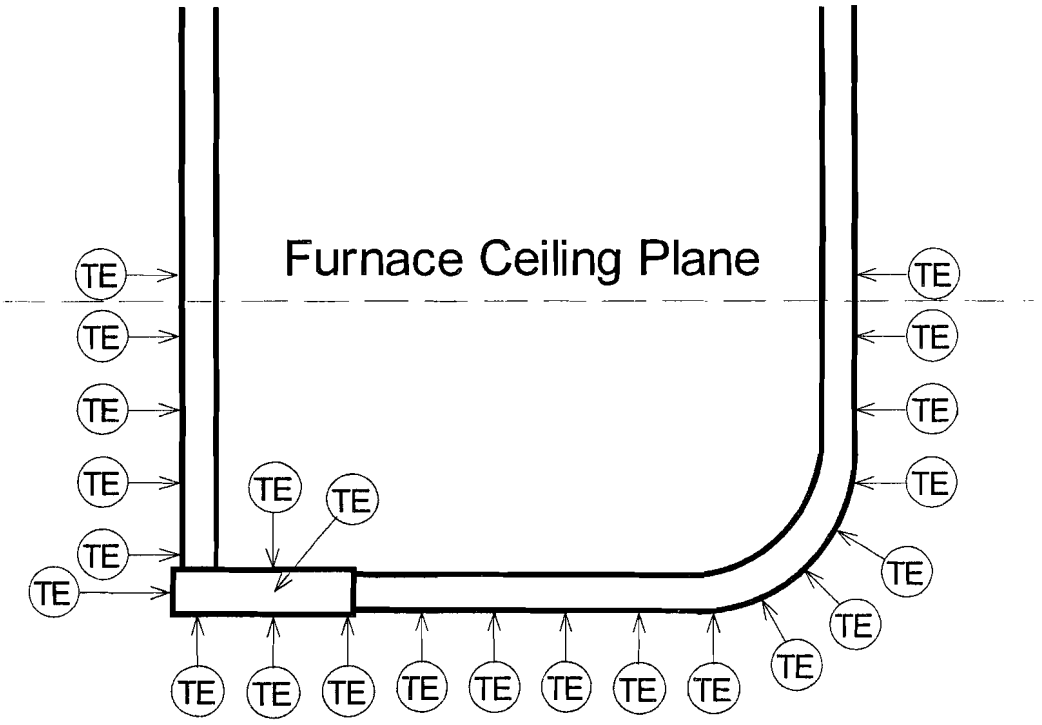


**Figure 9:** Planned Thermocouple Locations on the 63-mm (2½ in.) Conduit/Condolet LB Test Specimens. Note that at least one thermocouple will be attached to each face of the condolet LB fitting. A single bare copper wire (8 AWG) will be instrumented with thermocouples and routed inside the test specimen.

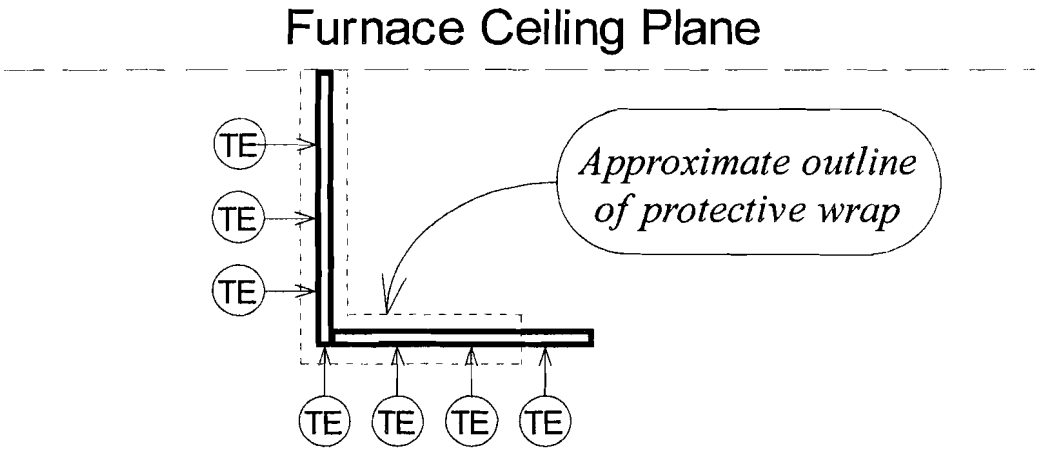


**Figure 10:** Planned Thermocouple Locations on the Partially Wrapped Support Structure Test Specimens.

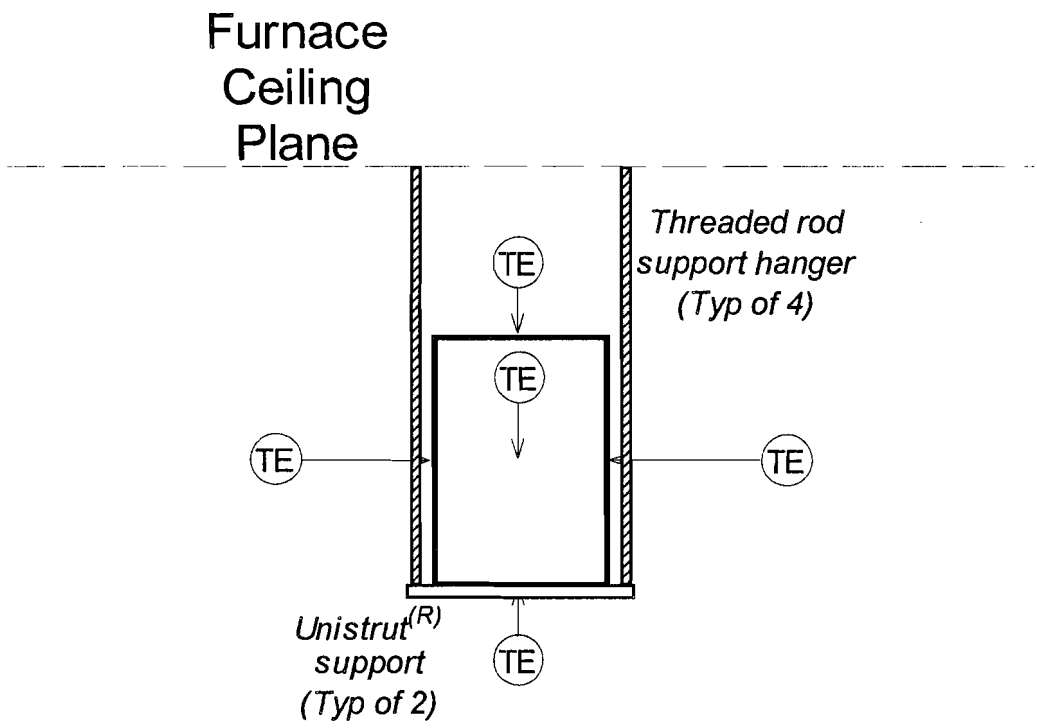


**Figure 11:** Planned Thermocouple Locations on the 30 cm x 61 cm x 25 cm (12 in. x 24 in. x 10 in.) Junction Box during Test #2. A thermocouple will be attached to each face of the junction box (6 total).

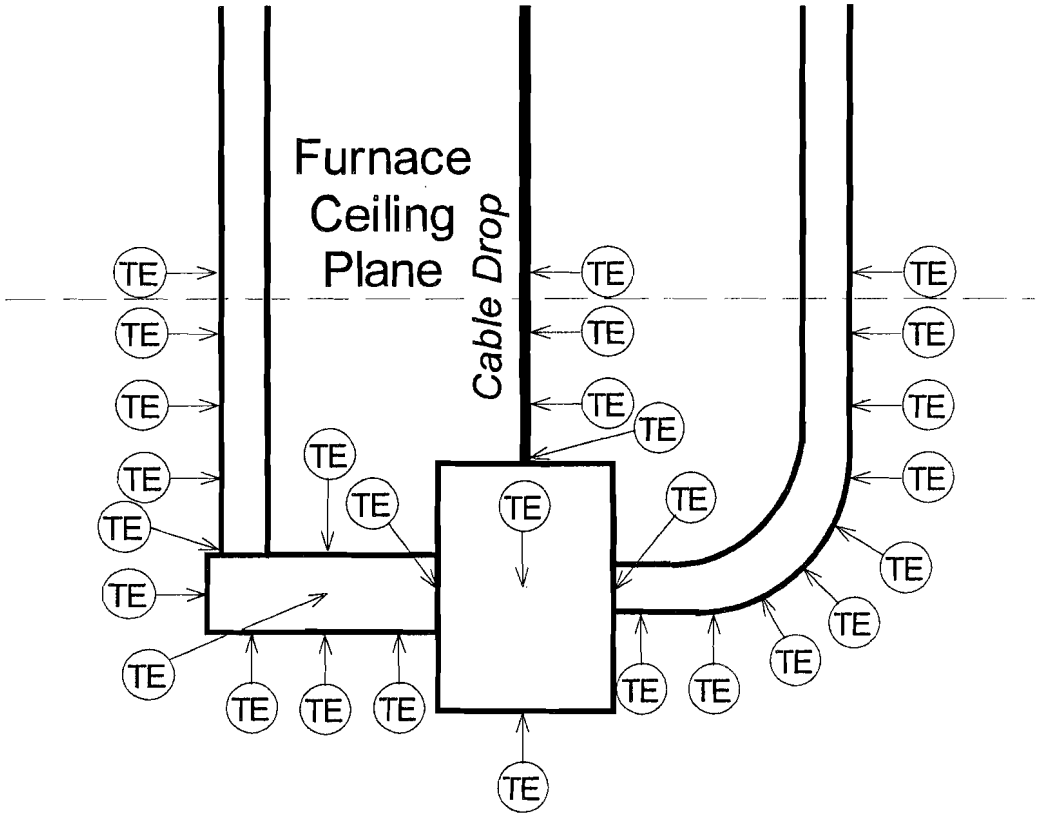


**Figure 12:** Planned Thermocouple Locations on the 103-mm (4 in.) Conduit and Junction Box/Cable Drop assemblies during Test #3. The cable drop will consist of a single bare copper wire (8 AWG) to which the thermocouples are attached. A thermocouple will also be attached to each of the six sides of the junction box.

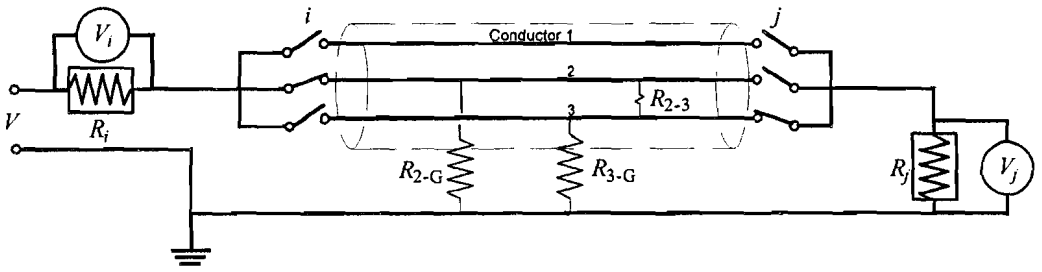


**Figure 13:** Schematic of the Insulation Measuring Circuit Showing Potential Leakage Current Paths.

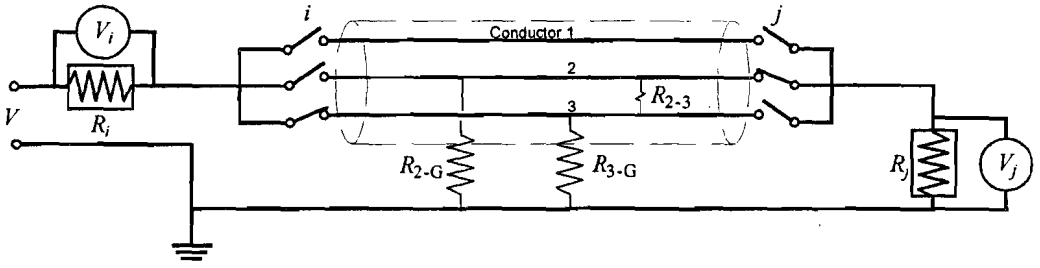


**Figure 14:** Complementary Insulation Measuring Circuit with Respect to the Circuit Shown in Figure 11.

# APPENDIX
## Research Program Considerations

The following items should be considered for inclusion in the test program to provide a research basis for the planned tests. Many of these recommendations were provided by industry comments received via letter.[1] The following list of considerations were not included in the revised fire barrier performance testing program plan because they did not fit in well with the very limited objectives of the NRR program. However, they should be given consideration in broadening the scope and objectives of a RES program.

**Fire Barrier Performance Model Development** – It would be beneficial to tailor the test program such that one principal outcome is the development of a mathematical model, based on the test data, that could estimate the expected performance of fire barriers that might differ from the tested configurations. The development of such a model would require a significant effort to include a variety of protected raceways so that the data and resulting model(s) would be applicable to a wide range of applications.

**ANI Test Protocols and Multiple versus Single Raceways** – The ANI Test Protocals test using a 'one layer' cable fill and circuit continuity. The current test protocal only tests single raceways not multiple raceways. The variety of cables, circuit voltages and raceway configurations used in actual plant configurations is diverse, and it would be difficult to consider a representative sample of cables, circuit voltages and multiple raceways within the same wrap in this test's scope. Such tests (using cable loading, energized circuits and multiple raceways) would likely be useful in developing a model to estimate expected fire barrier performance (see above).

**Multiple Wrap Thicknesses** – This test would test similar raceways in a variety of protective fire wrap thicknesses (e.g., 25-mm, 38-mm, 50-mm and 76-mm [1 in., 1½ in. 2 in. and 3 in.]). This test would provide a basis for assessing the effectiveness of a particular fire wrap based on applied thickness.

**Industry Review and Observation** – Consideration should be given to the industry's request that they be allowed to review and comment on the final test plan and detailed test specimen construction plans. They have also requested to be invited to be present to observe the construction of the test specimens, installation of the fire barriers and the conduct of the tests. Such involvement by industry representatives would be useful in that any potentially controversial issues concerning the fire barrier performance tests will be identified early and can be resolved in a timely manner.

---

[1]Letter: Marion, NEI, to Hannon, NRC/NRR, "Comments on NRC Hemyc Test Plan," December 6 2002.

# Risk Significance of HEMYC® Electrical Raceway Fire Barrier System Failures

Raymond H.V. Gallucci, Ph.D., P.E.

*U.S. Nuclear Regulatory Commission, MS O-11 A-11, Washington, D.C. 20555, rhg@nrc.gov*

## INTRODUCTION[a]

Approximately fifteen U.S. nuclear power plants (NPPs) employ the HEMYC® Electrical Raceway Fire Barrier System (HERFBS) to protect circuits in accordance with Nuclear Regulatory Commission (NRC) requirements [1]. Recent testing via Standard ASTM-E119 [2] indicated failures to achieve a one-hour fire rating [3-5]. We present a scoping analysis of the potential risk significance.

## PROBABILISTIC MODEL FOR TEST RESULTS

Failures resulting from shrinkage/tearing of the HERFBS covering were observed ≥15 min into the one-hour test, suggesting the following probabilistic model:

1. The HERFBS failure probability (P) for the ASTM-E119 fire ranges from 0 at ≤10 min to 1 at ≥60 min.

2. P is a function of the temperature "T" at time "t" or the area "A" at time "t" under the ASTM-E119 curve, whichever is more severe.

We linearized the ASTM-E119 curve (Fig. 1) and postulated failure thresholds of T = 704 °C and A = 4870 min-°C at t = 10 min, i.e.:

$$P(T[t]) = (T[t] - 704)/(920 - 704) \quad (1)$$

$$P(A[t]) = (A[t] - 4870)/(46470 - 4870) \quad (2)$$

where T = 920 °C and A = 46470 min-°C at t = 60 min.[b]

## ANALYSIS FOR TYPICAL NUCLEAR POWER PLANT FIRES

The HERFBS will not fail if T ≤ 704 °C, which bounds the temperatures reached by NPP fires where HERFBS is typically installed. However, NPP fires can expose a HERFBS to sufficiently high temperatures for long enough times to exceed the threshold A = 4870 min-°C. Fig. 1 shows a linearized CFAST® [6] simulation of an Emergency Diesel Generator (EDG) room oil fire with a rapid rise to T = 390 °C at t = 7.5 min and final T = 440 °C at t = 60 min, where the threshold value for A occurs at t = 16 min. At t = 60 min, A = 23250 min-°C and P(A) = 0.442 from Eq. (2).

Assume an older NPP uses a HERFBS for safe shutdown cables in their EDG room to protect against an oil fire,[c] with fast-acting smoke detection and pre-action/deluge sprinkler suppression. Based on the Fire Protection Significance Determination Process (FPSDP) [7], a medium loading of cables, two general electrical cabinets and one EDG yield a fire frequency = 4.8E-4/y + (2)(6.0E-5/y) + 0.0056/y = 0.0062/y. Conservatively we choose the FPSDP's more limiting severity characteristics and manual suppression curves -- "Indoor Oil-Filled Transformer" and "Turbine-Generator" (T-G) fires -- as surrogates for an oil fire severe enough to fail the HERFBS.

The FPSDP recommends a severity factor of 0.1. If we assume that the HERFBS damage fails any enclosed cables, it likely warrants nothing lower than 0.1 for conditional core damage probability (CCDP). We then express the core damage frequency (CDF) as 0.0062/y x 0.1 x 0.1 x P(A) x PNS = 6.2E-5/y x P(A) x PNS, where PNS is the non-suppression probability. For CDF ≤ 1E-6/y, we require P(A) x PNS ≤ 0.016.[d]

We expect rapid smoke detection; and, from the FPSDP, the non-suppression probability for the pre-action/deluge sprinklers is essentially zero, since the time-

[a] This paper was prepared by an employee of the U.S. NRC. The views presented do not represent an official staff position. Supporting material is available in NRC ADAMS (Accession # ML051300052).

[b] These failure temperatures refer to "furnace" temperatures, as per Standard ASTM-E119. The HERFBS covering begins to shrink at surface temperatures around 200 °C, but the shrinkage/tearing apparently does not translate into HERFBS failure as defined by ASTM-E119 until furnace temperatures exceed 700 °C [8, 9].

[c] If a plant were to lose both offsite and emergency onsite AC power due to a fire in the EDG room (station blackout), it would have an alternate means in place to safely shut down, independent of the EDGs or any other equipment in the EDG rooms.

[d] "When the calculated increase in CDF {which cannot exceed the CDF itself} is very small {i.e., < 1E-6/yr} ... the change will be considered {acceptable}" [10]. This "very small change" is typically accepted as a threshold for low risk significance.

to-damage (at least 16 min) minus the time-to-suppression (within 1 min) ≥ 10 min. The FPSDP recommends a 0.05 unavailability for a deluge system, thereby requiring manual suppression by the plant fire brigade 5% of the time. PNS for "T-G" fires, including this unavailability, = 0.05/exp([0.021][Δt]), where Δt ≈ t is the difference between times-to-damage and detection. The product P(A) x PNS rises from 0 at t = 16 min to 0.00627 at t = 60 min. Thus, it satisfies P(A) x PNS ≤ 0.016, yielding a maximum CDF = (6.2E-5/yr)(0.00627) = 3.9E-7/y.

### Sensitivity Case

For sensitivity, we assumed that P(T) and P(A) inversely varied quadratically and quartically to represent a rapid rise in the probability of HERFBS failure, followed by a gradual increase. We then calculated the maxima for P(A) x PNS and corresponding maximum CDFs shown in Table I. Even under these conservative bounding assumptions, we essentially satisfy P(A) x PNS ≤ 0.016 for CDF ≤ 1E-6/y.

### Other Nuclear Power Plant Fires

The preceding analyses were repeated for two other typical NPP fires, in an electrical switchgear room and make-up pump room. Each linearized CFAST® time-temperature curve, shown in Fig. 1, is less severe than that for the EDG room fire. Table I summarizes these parallel analyses, each of which yields lower CDFs than its EDG room fire counterparts.

## CONCLUSIONS

Within the assumptions of this analysis, which included conservatism from the FPSDP, the CDF due to recently indicated failures of the HERFBS appears to be bounded at 1E-6/y for typical NPP fires. This suggests a potentially low level of risk significance.[e]

## REFERENCES

1. U.S. Code of Federal Regulations, Title 10 (Energy), Part 50 (Domestic Licensing of Production and Utilization Facilities), Appendix R (Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979), Office of the Federal Register, Washington, DC (2005).

2. ASTM-E119-04, "Standard Test Methods for Fire Tests of Building Construction and Materials," ASTM Fire Test Standard, Sixth Edition, American Society of Testing and Materials, West Conshohocken, Pennsylvania.

3. U.S. NUCLEAR REGULATORY COMMISSION, *Information Notice 2005-07 – Results of HEMYC® Electrical Raceway Fire Barrier System Full Scale Testing*, U.S. Nuclear Regulatory Commission, Washington, D.C. (2005) [ADAMS Accession # ML050890089].

4. D. PRIEST, C. HUMPHREY, *HEMYC® (1-Hour) Electrical Raceway Fire Barrier Systems Performance Testing – Conduit and Junction Box Raceways*, Omega Point Laboratories, Inc., Elmendorf, Texas (2005) [ADAMS Accession # ML051190014].

5. D. PRIEST, C. HUMPHREY, *HEMYC® (1-Hour) Electrical Raceway Fire Barrier Systems Performance Testing – Cable Tray, Cable Air Drop and Junction Box Raceways*, Omega Point Laboratories, Inc., Elmendorf, Texas (2005) [ADAMS Accession # ML051190096].

6. R. PEACOCK, W. JONES, G. FORNEY, *CFAST: Consolidated Model of Fire Growth and Smoke Transport (Version 5), User's Guide*, NIST SP 1034, National Institute of Standards and Technology (NIST), Gaithersburg, Maryland (2004).

7. U.S. NUCLEAR REGULATORY COMMISSION, "Fire Protection Significance Determination Process," *Inspection Manual Chapter 0609, Appendix F*, U.S. Nuclear Regulatory Commission, Washington, D.C. (2004).

8. B. LEVIN, "Documents Supporting HEMYC® Tests and Insulation Fabrication," April 12, 2005, Letter to F. Wyant, Sandia National Laboratories, Albuquerque, New Mexico (2005) [ADAMS Accession # ML051190055].

9. HAVEG INDUSTRIES, INC., *SILTEMP® Thermal Barrier Technical Bulletin HS-116*, Wilmington, Delaware (1982).

10. U.S. NUCLEAR REGULATORY COMMISSION, *Regulatory Guide 1.174 – An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*, Revision 1, U.S. Nuclear Regulatory Commission, Washington, D.C. (2002).

[e] This analysis is illustrative only. Plant-specific conclusions should be based on actual plant conditions and plant-specific analyses.

TABLE I. Analysis Results for Three Typical Nuclear Power Plant Fires in Areas Employing HERFBS

| | EDG Room (Oil Fire) | | Electrical Switchgear Room | | Make-up Pump Room | |
|---|---|---|---|---|---|---|
| | Combustible | Frequency | Combustible | Frequency | Combustible | Frequency |
| Analysis Parameters | Cables (medium loading) | 4.8E-4/y | Cables (high loading) | 0.0014/y | Cables (low loading) | 1.6E-5/y |
| | General electrical cabinets (2) | (2)(6.0E-5/y) = 1.2E-4/y | Electrical switchgear (25) | (25)(6.0E-5/y) = 0.0015/y | General electrical cabinets (2) | (2)(6.0E-5/y) = 1.2E-4/y |
| | Diesel generator | 5.6E-4/y | | | Pumps (6) | (6)(1.0E-4/y) = 6.0E-4/y |
| | Total | 0.0062/y | Total | 0.0029/y | Total | 7.4E-4/y |
| | Fire Severity[f] | Indoor oil-filled transformer | Fire Severity[f] | Large electrical fires | Fire Severity[f] | Large electrical fires |
| | Manual suppression curve | Turbine-generator fires | Manual suppression curve | Energetic arcing fault | Manual suppression curve | All (fire) events |
| | PNS | 0.05/exp(0.021t) | PNS | 0.05/exp(0.051t) | PNS | 0.05/exp(0.069t) |
| | CCDP | 0.1 | CCDP | 0.1 | CCDP | 0.1 |
| | Maximum P(A) x PNS (allowed) | 0.016 | Maximum P(A) x PNS (allowed) | 0.034 | Maximum P(A) x PNS (allowed) | 0.14 |
| Base Case (Linear) | Maximum P(A) x PNS (calculated) | 0.00627 (at t = 60 min) | Maximum P(A) x PNS (calculated) | 0.00104 (at t = 37.5 min) | Maximum P(A) x PNS (calculated) | 2.2E-4 (at t = 40 min) |
| | CDF | 3.9E-7/y | CDF | 3.0E-8/y | CDF | 1.7E-9/y |
| Sensitivity Case (Quadratic) | Maximum P(A) x PNS (calculated) | 0.0105 (at t = 40 min) | Maximum P(A) x PNS (calculated) | 0.00322 (at t = 27.5 min) | Maximum P(A) x PNS (calculated) | 9.57E-4 (at t = 32.5 min) |
| | CDF | 6.5E-7/y | CDF | 9.3E-8/y | CDF | 7.1E-9/y |
| Sensitivity Case (Quartic) | Maximum P(A) x PNS (calculated) | 0.0162 (at t = 27.5 min) | Maximum P(A) x PNS (calculated) | 0.00674 (at t = 22.5 min) | Maximum P(A) x PNS (calculated) | 0.00237 (at t = 30 min) |
| | CDF | 1.0E-6/y | CDF | 2.0E-7/y | CDF | 1.8E-8/y |

[f] The fire severity factor = 0.1.

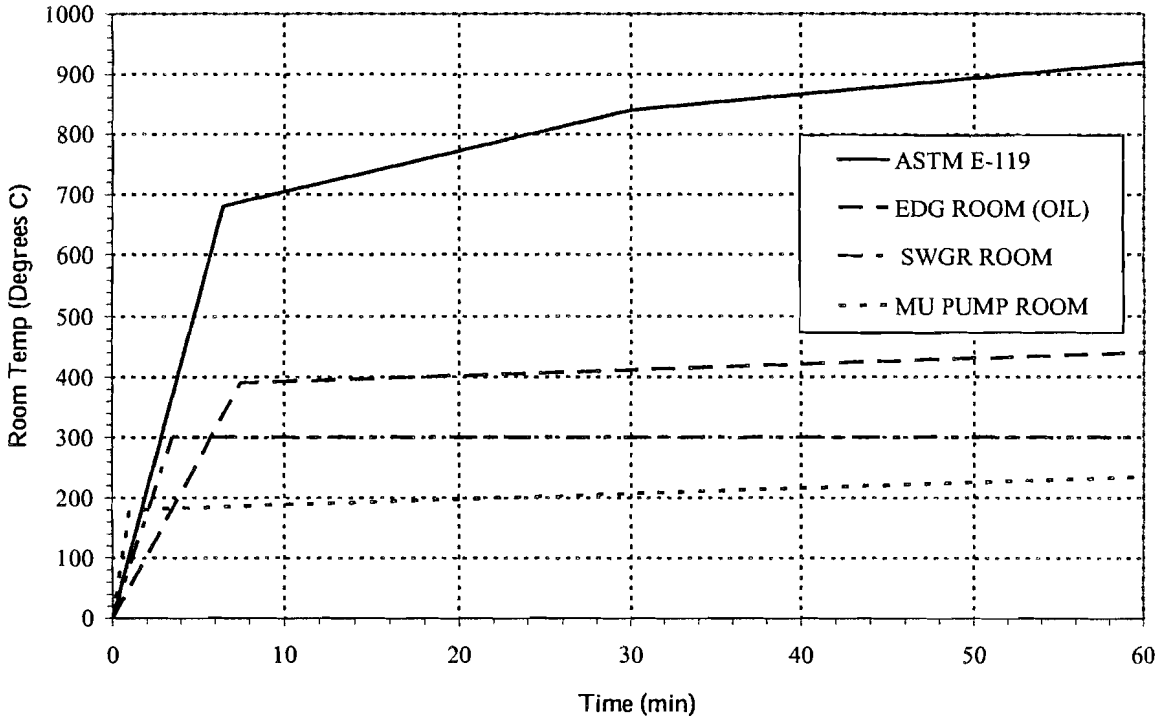


FIGURE 1. Linearized CFAST Time-Temperature Curves for Selected NPP Fires
(Note: Shrinkage of HERFBS Covering Begins at SURFACE Temp ~ 200 C)

368

ɔogo.org POGO Letter to NRC Chairman Niles Diaz 12/9/2003 Project On Government Oversight

December 9, 2003

POGO Letter to NRC Chairman Niles Diaz

December 9, 2003

Chairman Niles J. Diaz
Nuclear Regulatory Commission
11555 Rockville Pike
Rockville, MD 20852

Via facsimile: (301) 415-1757

Dear Chairman Diaz,

As you recall, in September I wrote to you to respond to your letter to the New York Congressional delegation and local politicians claiming that this summer's force-on-force test at Indian Point had shown a "strong defensive strategy and capability." The NRC responded to my letter by demanding that POGO not make the letter public, claiming that it contained homeland security sensitive and "safeguarded" material. The NRC threatened us with civil and criminal sanctions were we to continue to make public either our letter or any of the sensitive material it allegedly contained. The NRC also took the position that it had no obligation to identify the passages in the letter that it claimed were sensitive. As a result, the NRC's initial position was that any effort by POGO to criticize the lack of security at Indian Point threatened the release of safeguards information and thus POGO did so at the risk of criminal prosecution. We believe that the agency took this position to stifle legitimate criticism of the agency by POGO.

We did not let the matter end there. POGO retained counsel and threatened legal action against the NRC for stifling POGO's speech. Ultimately, the agency backed down and agreed to identify the portions of our September letter that were in the agency's view problematic. We appreciate the

369

agency's willingness to engage POGO on this issue and believe that our discussions were helpful to all concerned. What follows is a redraft of our original letter. We look forward to your prompt response.

Our primary concern is that the way the force-on-force (FOF) tests were conducted do not give you the ability to reassure the public that the Indian Point security force has been proven capable to defend that facility against a credible terrorist attack. After a thorough review of the test of security at Indian Point, we continue to have the following concerns:

Dumbed-Down Design Basis Threat (DBT) – It has been widely reported in the press1 that prior to 9/11, nuclear power plants were required to have defenses designed to protect against only a ridiculously small attacking force – three terrorists. In contrast, the intelligence community generally believes that terrorists would attack a target with a squad-sized force, which in the Army special forces is 12 and the Navy Seals is 14. In other words, the NRC would need to at least quadruple its old DBT.

Having interviewed a number of people who have reviewed the NRC's new DBT, we do not believe that it is even close to reaching the 12 to 14 level we believe is appropriate. Representatives of other federal agencies have told POGO that the NRC's new DBT remains inadequate.

The NRC argues that the new DBT is the largest threat against which a private security force can be expected to defend. This rationale is backwards and conflates two separate considerations – what is the size of the threat and what should the nuclear power industry be required to do to in the face of such threats. The NRC policy decision to limit the size of the DBT (under terrific pressure from the nuclear industry and its friends in Congress) was based mainly on its assessment of what is reasonable to ask of a private force. But that approach ignores the most fundamental question: what is the credible threat against the facilities? The size of the DBT must be based on that threat. Furthermore, NRC's justification of its too-low DBT rings hollow, as the Department of Energy (DOE) also relies on a private security force, yet at some facilities, DOE claims to protect its facilities against twice as many terrorists as the NRC does.

Under Use of Readily-Available Lethal Weapons – It is well known in security circles that there are weapons that are available to terrorists that can penetrate bullet-resistant enclosures (BREs), which are quasi-guard towers. BREs are included in the defensive strategy of a

370

number of nuclear power plants, including Indian Point. Some time ago, the Department of Energy abandoned the use of its state-of-the-art guard towers (which are far more robust than most BREs) because of their vulnerability to readily-available weapons. Indian Point officers have been aware of the controversies surrounding BREs and have brought their concerns not only to Entergy, but also to the NRC Region I, with no response at all. Several years ago, the DOE developed a classified official Adversary Capabilities List which includes weapons and explosives that are readily available to terrorist groups. The NRC should review this list and ensure its Design Basis Threat includes them. For example, .50 caliber sniper rifles (which have been available since World War I) and Armor-Piercing Incendiary rounds (which are available in gun shops for $1 per round) made the DOE guard towers so vulnerable they were abandoned. Other weapons were also of concern, including the rocket-propelled grenades which have been used frequently by near-children around the world in war-torn countries, with great success against hardened targets.

Unrealistic Timing and Location of Attack – It appears the NRC conducted the three FOF tests at Indian Point during the daylight at the beginning of the night shift, and began at least two of the tests in the owner-controlled area. There are several problems with this:

The security force being tested had just come on duty and was not yet fatigued by a 12-hour shift, hours typically worked by Indian Point security officers five to six days a week.

The security officers knew within the hour that the test was to begin, as the day shift was held over an extra hour to cover as a shadow force so that the night shift could be tested at the beginning of their shift.

It is widely believed in the intelligence community that no one will attack during daylight, as it is to the attacker's advantage to have the cover of darkness. Despite this, all three FOF tests occurred between 4-6 pm. Furthermore, in two of the three tests, the mock terrorists were required to cross open fields in broad daylight in order to reach the protected area, making it that much easier for them to be observed by the security officers.

The mock terrorists attacked from only one entry point. In addition, the NRC and Entergy agreed that, if the attackers were successful in reaching the protected area fences, there would be a halt in the action

371

and the adversaries would be brought inside of the fences (to prevent any actual damage to the fences during the exercise) – making it perfectly obvious from where the attack will be coming. POGO had previously alerted the NRC to a particular vulnerability involving the fences at most nuclear facilities and was assured that this vulnerability would be taken into account in future FOF tests. However, it was does not appear to have been taken into account during the Indian Point FOF.

Amateur Mock Terrorists – A terrorist group has advantages that cannot be replicated in even the best mock attack FOF. However, the following limitations could have been partially ameliorated by the NRC, but were not:

No Surprise. The security force knew for months in advance that this test was going to occur, training specifically for the approved scenarios. They even knew within minutes that the test was to occur, because of all the visiting dignitaries and the fact that they had strapped on Multiple Integrated Laser Engagement System (MILES) equipment.

No Violence of Action. During a mock FOF there is no real danger – no live ammo, no colleagues dying or being maimed or any other adverse impact that would normally create chaos and in some cases cause the protective forces to panic. As a result, security forces develop "MILES bravery."

Safety First. The FOF tests are not conducted at high speed because of the overriding safety concerns. Therefore, people and vehicles are not going full tilt the way they would during a real terrorist attack, giving the protective forces time to pause to make decisions – time that they wouldn't have in a real life situation. Safety was also used as the reason for not conducting the tests at night. Sources told us that Entergy was worried participants could trip over rocks or step on snakes.

No Trained Adversaries. The mock terrorists were security officers from another nuclear plant who had no training as adversaries. This training is critically important because it teaches the mock terrorist how to think and act offensively, as a real terrorist would, rather than defensively as a security guard would. Here again, both DOE and the

372

military use trained adversaries to test their security forces.
The Security Forces Are On Their Own – It should be recognized that although the exercise was observed by the State Police and FBI, these law enforcement entities cannot respond to an attack with SWAT capability before it is too late. Insofar as we know, these response times have not been tested at Indian Point. But tests at other facilities have shown that an attack is generally won or lost in between three and eight minutes, while it generally takes an hour or two for SWAT teams to respond.

Poor Planning: Lives at Risk – One of the FOF tests was quickly aborted when Coast Guard personnel, who had not been previously informed that the test was to occur, threatened to use their live ammo against the mock attackers. It is unacceptably poor planning to allow this kind of lack of professionalism, putting lives at risk.

Recommendations:

The NRC should:

Not allow so much advanced notice and training for the FOF – two weeks is sufficient;

Make the window of attack much less obvious, therefore making it unclear to the participants at what time during the shift the test will take place;

Administer most of the tests when it is dark;

Use trained adversary teams from the military or develop its own trained adversary team;

Conduct computer simulations – either Joint Tactical Simulations (JTS) or Joint Conflict Adversary Tactical Simulations (JCATS) – used by the military and Department of Energy for years. These computer programs simulate the movement of personnel through architecturally- and terrain-accurate models of the facility. This preparation helps the security forces develop the best strategies for defeating any number of possible attacks;

319

Include the use of simulated rocket-propelled grenades, sniper rifles with .50 caliber armor-piercing incendiary rounds, gas, smoke and other commonly used weapons and diversionary devices if they are not currently in the DBT; and

Address the serious communications breakdowns that occurred during the recent Indian Point FOF.

These issues are obviously very serious and need to be addressed promptly. We look forward to your response.

Sincerely,

Danielle Brian
Executive Director

cc Roy Zimmerman

1. U.S. News & World Report, September 17 2001; Chicago Tribune, July 12, 2002; The Boston Globe, May 14, 2002; Bulletin of the Atomic Scientists, January 1, 2002; New York Times Magazine, May 26, 2002.



---

374

March 27, 2007

Re: NRC Proposed Rule: Power Reactor Security Requirements (RIN 3150-AG63)

Annette Vietti-Cook, Secretary
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Attn: Rulemakings and Adjudications Staff
Submitted via e-mail to SECY@nrc.gov

COUNCIL ON INTELLIGENT ENERGY & CONSERVATION POLICY (CIECP) COMMENTS TO PROPOSED RULE 10 CFR PARTS 50, 72 AND 73 REGARDING POWER REACTOR SECURITY REQUIREMENTS AT LICENSED NUCLEAR FACILITIES

Nearly six years after September 11, 2001, the 103 civilian nuclear reactors in the United States are still not in a position to repel attacks by adversaries with capabilities commensurate with those of either the 9/11 terrorists or with enemies of the United States currently operative on the world stage. The present Power Reactor Security Requirements (PRSR) thus fall far short of the actual threat level faced by the U.S. today, much less the escalated level the nation will face as nations such as Russia, China and Iran improve and export nuclear engineering expertise. Indeed, as numerous security experts have pointed out, a terrorist group with access to sympathetic nuclear scientists and engineers would have sufficient sophistication to target the critical systems and weak links of nuclear reactors. The assistance that Pakistani nuclear scientists reportedly offered to Al Qaeda illustrates this threat.

Recent National Intelligence Estimates and National Intelligence Council Reports describe the terrorist threat to the U.S. as real and as having no sign of abatement for many years to come. These reports further warn of a new class of â€œprofessionalizedâ€• terrorists -in part created by the Iraq war- who must be expected to have strong technical skills and English language proficiency. Such individuals should, in the future, be expected to become major players in international terrorism.

Al Qaeda and other terrorist groups have shown extraordinary tactical ingenuity and a complete lack of reverence for human life. Further there is ample evidence that U.S. nuclear power plants, particularly those sited near metropolitan areas, are viewed as attractive terrorist targets. Notably, the 9/11 Commission learned that the original plan for a terrorist spectacular was for a larger strike, using more planes, and including an attack on nuclear power plants. In an Al-Jazeera broadcast in 2002, one of the planners of 9/11 said that a nuclear plant was the initial target considered. We also know from the 9/11 Commission's investigation that, even after the plot was scaled down, when Mohammed Atta was conducting his surveillance flights he spotted a nuclear power

315

plant (unidentified by name, but obviously the Indian Point nuclear power plant) and came close to redirecting the strike. National Research Council analyses and post-9/11 intelligence has also indicated that the U.S. nuclear infrastructure is viewed as an alluring target for a future terrorist spectacular. As the Chairman of the National Intelligence Council stated in 2004, nuclear power plants â€œare high on Al Qaeda's targeting list,â€• adding that the methods of Al Qaeda and other terrorist group may be â€œevolving.â€•

There is, thus, every reason to believe that a sizable, well-planned and orchestrated military operation against a U.S. nuclear facility is well within both present and near-future terrorist intent and capability. In view of these realities, the current proposed PRSR is utterly inadequate.

Consequently, the COUNCIL ON INTELLIGENT ENERGY & CONSERVATION POLICY (CIECP) urges the NRC to address the following realities in its PRSR:

ACTIVE INSIDERS

The voluminous number of security breaches which have occurred at critical infrastructure, including nuclear weapons and power facilities after 9/11 (such as the 16 foreign-born construction workers who were able to gain access to the Y-12 nuclear weapons plant with falsified documentation) demonstrates that nuclear â€œinsidersâ€• must be deemed potential active participants in an attack.

This threat is significantly augmented by nuclear power plant operators' increasing outsourcing of on-site work in order to cut costs.

Contractor oversight failures have been documented by the NRC. For example a December 22, 2003 NRC Special Inspection Report on the Indian Point Nuclear Generating Station in Buchanan, New York (Indian Point) operated by Entergy Nuclear Northeast (Entergy) notes â€œthe common theme of a lack of direct contractor oversight and quality control measures, along with the absence of Entergy subject matter experts to independently assess contracted work activitiesâ€¦.â€• Critically, the risk of sabotage is elevated at all power plants during periods of refueling and major construction work when hundreds of outside contract workers have site access.

The active participation of insiders, including contract workers, in a terrorist offensive need not take place during the time of attack. It may occur days or even many months prior to an attack. In addition to actions such as surveillance of plant schematics, security features and protocols, pre-attack participation may involve the sabotage of critical instrumentation, computers, piping, electronic systems or any number of other components, where such sabotage would likely not be discovered prior to an emergency event.

316

## COMPUTER SYSTEM COMPROMISE

Nuclear power plant computer systems, like those of other critical infrastructure, are subject to a range of vulnerabilities, including power outages, attacks by malicious hackers, viruses and worms. Compromise of integrity may also occur at the level of software development via backdoors written into code or the implantation of logic bombs programmed to shut down a safety system at a particular time.

Many terrorist networks have the resources and technical savvy to wreak havoc. For example, the alleged terrorist, Muhammad Naeem Noor Khan, picked up in Pakistan in 2004, and believed to have links with Al Qaeda, is a computer engineer.

The fact that U.S. nuclear reactors are not impregnable was demonstrated by the penetration of the Slammer worm into the Davis-Besse nuclear facility. That intrusion disabled a safety monitoring system for nearly 5 hours. In addition, computer hackers have broken into U.S. Department of Energy computers. Some of such intrusions were root-level compromises, indicating that hackers had enough access to install viruses.

Computers at nuclear power stations are also vulnerable to acts of sabotage against off-site power transmission, as was evidenced at Indian Point during the 2003 blackout which struck the Northeast. At Indian Point, various computer systems had to be removed from service, including the Critical Function Monitoring System, the Local Area Network, the Safety Assessment System/Emergency Data Display System, the Digital Radiation Monitoring System and the Safety Assessment System.

It is, accordingly, a matter of pressing importance that the NRC engage independent experts to develop a comprehensive computer vulnerability and cyber-attack threat assessment. Such an assessment must evaluate the vulnerability of the full range of nuclear power plant computer systems and the potential consequences of such vulnerabilities. The PRSR must incorporate such findings and include a protocol for quickly detecting such an attack and recovering key computer functions in the event of an attack.

## CHEMICAL WEAPONS

The PRSR must fully address the potential consequences of the use of toxic chemicals as part of an attack scenario. There are numerous agents that can be deployed with almost instantaneous effect and can immobilize targets via paralysis, convulsions, blinding, suffocation or death. Such agents could be employed as part of the initialization strategy. For, example, a truck or even large SUV filled with chlorine, boron trifluoride, hydrofluoric acid, liquid ammonia, or any number of other agents could be crashed into a perimeter

barrier, with the resulting fumes killing or disabling plant personnel guarding the outdoor area of the facility.

Chemical agents could also be introduced surreptitiously into building ventilation systems. They may also be used strategically to neutralize workers endeavoring to maintain control of the situation.

Many such agents are easy to make and do not require sophisticated delivery systems. Some can be carried in coffee mugs or in vials within body cavities. Phenarsazine chloride, an arsenic derivative, can be transported in minute quantities, even as a powder that can be dusted on paper. It is lethal if burned and even a spoonful can cause immediate extreme irritation of the eyes and breathing passages. A chemical like chloroform ascitone methanol can be transported on filter paper, then combined with a heat source to create an explosion.

CONVENTIONAL WEAPONRY

Intelligence and military analysts have repeatedly warned that extremists in Iraq, the tribal areas of Pakistan and elsewhere are currently developing a high level of military skill and experience. This reality underscores the need for nuclear plants to be able to defend against attackers utilizing the full range of potential weaponry that terrorists are known to be capable of using, including heavy caliber automatic weapons; sniper rifles; shoulder-fired rockets; mortars; platter charges; anti-tank weaponry; bunker busters; shaped charges; rocket-propelled grenades; and high-power explosives.

Numerous weapons systems posing a threat to even the best trained and equipped civilian guard force, as well as to on-site installations, are readily available and easy to transport. To wit:

o Assault rifles and other rapid-fire battlefield weapons such as AK-47's, Uzi's and TEC-9's are freely available in the U.S. A weapon like the SKS 7.62-millimenter semiautomatic assault rifle can be purchased for under $200. In 2005 the Government Accountability Office reported that 47 individuals on a federal terrorism watch list were actually permitted to legally buy guns in 2004.

o A standard M-24 sniper rifle with day and night scope can be carried in a canvas bag and fires 7.62-millimeter ammunition targeting up to 3000 feet

o A .50-caliber Barrett rifle, which can be purchased for $1000 on the internet, weighs a mere 30 lbs and can hit targets up to 6000 feet away with armor-piercing bullets that can blow a hole through a concrete bunker, bring down a helicopter or pierce an armored vehicle.

o A rocket propelled grenade launcher is re-loadable, can fire at the speed

378

of 400 feet per second and can blow a vehicle into the air.

o A TOW missile is an accessible form of military hardware used in over 40 countries and can be fired from a launcher on a flatbed truck. A 1998 test TOW fired into a nuclear waste transport cask (which is more robust than many on-site nuclear waste storage casks) blew out a hole the size of a grapefruit. The Kornet-E missile, developed by the Soviets and sold to Iraq, can travel over 3 miles and cut through over 3 feet of steel. The world's arms market is awash in thousands of Milan missiles. The 60-70 lb Milan missile system has an effective range of over 5000 feet and can blow a hole through more than 3 feet of armor plate.

o The deployment of increasingly powerful and sophisticated explosives, including shaped charges and explosively formed penetrators (or E.F.P.s) by terrorists and insurgents in Iraq show that the explosives use capabilities of enemies of the United States should not be underestimated. Notably, the 18 men arrested in Australia in November 2005, and believed to have been planning an attack on an Australian nuclear reactor, had allegedly been stockpiling materials used to make the explosive triacetone triperoxide, or TATP. Terrorists targeting a U.S. nuclear power plant may very well be able to draw on expertise developed during the Iraq insurgency as well as military experts and rocket scientists from the former Iraq government or from hostile nations such as Iran. In addition, the strategic utility of explosives is magnified when bombers are willing to blow themselves up. Suicide bombers able to gain access to the internal areas of a nuclear power plant during the course of an attack could cause untold destruction.

o Perhaps the most intractable military hardware threat is posed by shoulder-fired missiles such as Stingers, SA-7's, SA-14's and SA-18's. An estimated 500,000 such systems are scattered throughout the world and have been found in the possession of at least 27 terrorist or guerrilla groups. Some can be bought easily on the black market for as little as several thousand dollars each. Critically, shoulder-fired missiles are easy to operate (Al Qaeda training videos offer instruction) and are designed for portability, typically being 5-6 feet long and weighing 35 lbs. They can be transported by and fired from a van, S.U.V., pickup truck or recreational boat. Even a single terrorist armed with a shoulder-fired missile can cause immediate and substantial damage to a targeted structure. Traveling at more than 1,500 miles per hour, a typical shoulder-launched missile has a range of over 12,000 feet. If the target remains intact following the initial strike, the terrorist can attach a new missile tube to the grip stock launcher and fire again.

## WATERBORN ATTACKS

Waterborne defenses of nuclear plants adjacent to navigable waterways must be significantly enhanced. Facilities must either be engineered to withstand damage from a waterborne attack or suited with physical barriers that prevent

entry to the plant and/or critical cooling intake equipment.

Continual cooling is an essential component of nuclear plant safety. A meltdown can be triggered even at a scrammed reactor if cooling is obstructed. Water intake is also essential to the proper function of spent fuel pools. Yet at certain nuclear plants, cooling systems may be highly vulnerable. At both Indian Point and Millstone Power Station, in particular, water intake pipes have been identified by engineering experts as exposed and susceptible to waterborne sabotage.

One or more boats laden with high energy explosives could severely compromise cooling water intakes easily and quickly. Indian Point, for instance, is located on the banks of the Hudson River in an area heavily trafficked by commercial and recreational vessels. The 900 foot â€œExclusion Zoneâ€• -marked only by buoys- could be traversed by speed boats in 30 - 40 seconds, well before any Coast Guard or other patrol boat could react. Patrol boats could also be readily taken out by suicide bomber boats crashing into them (in the manner a small explosives laden boat targeted the destroyer the USS Cole in 2000) or by weaponry like shoulder-fired missiles or rocket propelled grenades.

AERIAL ASSAULT

According to a terrorist â€œthreat matrixâ€• issued by the National Research Council and the National Academies of Sciences and Engineering following the September 2001 attack, â€œNuclear power plants may present a tempting high-visibility target for terrorist attack, and the potential for a September 11-type surprise attack in the near term using U.S. assets such as airplanes appears to be high.â€•

In March 2005, a joint FBI and Department of Homeland Security assessment stated that commercial airlines are â€œlikely to remain a target and a platform for terroristsâ€• and that â€œthe largely unregulatedâ€• area of general aviation (which includes corporate jets, private airplanes, cargo planes, and chartered flights) remains especially vulnerable. The assessment further noted that Al Qaeda has â€œconsidered the use of helicopters as an alternative to recruiting operatives for fixed-wing operations,â€• adding that the maneuverability and â€œnon-threatening appearanceâ€• of helicopters, even when flying at low altitudes, makes them â€œattractive targets for use during suicide attacks or as a medium for the spraying of toxins on targets below.â€•

The vulnerability of nuclear power plants to malevolent airborne attack is detailed extensively in the Petition filed by the National Whistleblower Center and Randy Robarge in 2002 pursuant to 10 CFR Sec. 2.206. A number of studies of the issue are also reviewed in Appendix A to these Comments. The particular vulnerability of nuclear spent fuel pools to this kind of attack is detailed in the January 2003 report of Dr. Gordon Thompson, director of the Institute for Resource and Security Studies entitled â€œRobust Storage of Spent Nuclear Fuel: A Neglected Issue of Homeland Securityâ€• and in the findings of a

multi-institution team study led by Frank N. Von Hippel, a physicist and co-director of the Program on Science and Global Security at Princeton University and published in the spring 2003 edition of the Princeton journal Science and Global Security under the title â€œReducing the Hazards from Stored Spent Power-Reactor Fuel in the United States.â€• It is worthy of note that, even post-9/11, general aviation aircraft have circled or flown closely over commercial nuclear facilities without military interception.

The NRC's sole present strategy for averting a kamikaze attack upon a nuclear power plant is reliance upon aviation security upgrades implemented by the Transportation Security Administration and the Federal Aviation Administration and faith that U.S. intelligence will provide ample warning.

It is this kind of governmental agency pass-the-buck mindset that brought the nation Katrina.

The NRC's conjecture also betrays a reality disconnect reminiscent of the federal response to Katrina. Since 2001 there have been numerous breaches of airport security throughout the nation. Notably, in late 2005, there were three serious security breaches at Newark International Airport, one of the points of departure used by the September 11 hijackers. The most serious occurred on November 12, 2005, when a man driving a large S.U.V. barreled through the armed security checkpoint and drove in a secured area for 45 minutes before being found by NY/NJ Port Authority officers. Just this year, gaping holes in airport security were exposed when workers with access to secure areas were able to carry firearms in their carry-on bags onto a commercial jet departing from Florida.

The PRSR must furthermore be upgraded to include high-speed attack by a jumbo jet of the maximum size anticipated to be in commercial use (such as the expanded version of the Boeing 747 and the Airbus A380) as well as unexpected attack by general aviation aircraft and helicopters. The PRSR must contemplate all such aircraft to be fully loaded, fueled and armed with explosives.

It is essential that the PRSR address not only the direct effect of impact, but the full potential aftereffects of (A) induced vibrations; (B) dislodged debris falling onto sensitive equipment; (C) a fuel fire; and (D) the combustion of aerosolized fuel (especially in combination with pre-existing on-site gases such as hydrogen).

The PRSR must further take into consideration the cascading consequences of aerial assault on the full spectrum of plant installations. Inarguably, there is a wide range of on-site structures, not within hardened containment, that are critical to the safe operation of a nuclear plant. Spent fuel pools are of particular concern because the disposition of water could uncover the fuel. If plant workers are unable to effectuate replacement of the water (either because of fire or because they are otherwise incapacitated), experts warn, an exothermic reaction could cause the zirconium clad spent fuel rods to ignite a

nuclear waste conflagration that would very likely spew the entire radioactive contents of the spent fuel pool into the atmosphere.

Without question, hardening a nuclear power plant against aerial threat will necessitate significant upgrades in plant fortification. However even relatively modest measures such as the installation of Beamhenge and the placement of all sufficiently cooled spent fuel into Hardened On-Site Storage Systems (known as H.O.S.S.) would add measurable protection.

## STRATEGIC USES OF RIGS, TRUCKS AND S.U.V.'S

In June 1991, the NRC denied the truck bomb petition of the Committee to Bridge the Gap and the Nuclear Information Resource Service, on the grounds that it was not realistic to believe a truck bomb would be employed in the U.S. Two years later, on February 26, 1993, terrorists drove a rented van packed with explosives into the underground garage of the World Trade Center, lighted a fuse and fled. Just a couple of weeks before that, a mentally unstable individual crashed his station wagon through the gates of the protected area of the Three Mile Island nuclear power station and evaded security for several hours before finally wrecking his vehicle by crashing into the turbine building. Thereafter, the NRC reconsidered its earlier assessment and has, on a number of occasions, upgraded reactor security standard to include some protections against land vehicles. Such upgrades, however, are insufficient in a post-9/11 world.

Large Sport Utility Vehicles and pickup trucks on the road today can weigh over 8 tons, loaded, and -as do commercial vans- have considerably carrying capacity. Such vehicles could be used strategically in a number of ways.

The first is as a mobile short range projectile bomb. A large, heavy vehicle packed with high explosives, even if not successful in penetrating concrete barriers, could result in the death or incapacitation of large numbers of plant workers, including security, personnel. Such casualties would be particularly likely to materialize if the vehicle bomb followed a previous diversionary event intended to draw security personnel to the plant perimeter.

The second is as a transport vehicle for one team of attackers who are themselves armed or who wear explosive belts and could then themselves penetrate other areas of the facility. A terrorist wearing an explosive body belt can, in effect, be a precision guided weapon.

The third and fourth scenarios are variations of the first two, with chemical agents substituted for or combined with explosives. (Indeed, insurgents in Iraq are increasingly combining explosives with chlorine gas and other chemical payloads in truck bomb detonations.) One or two such vehicles packed with the right toxins, could be expected to kill or disable a substantial number of workers, again, especially if the release followed a prior event which drew security personnel to the area, or simply to areas outside facility enclosures.

382

Certain toxins can be lethal to anyone within miles. Using such agents, attackers wearing protective gear could then gain access to other areas of the facility.

A fifth tactical use of vehicles would not even occur on site. Vehicles carrying explosives and/or chemical agents could be set off at critical regional transportation arteries such as major bridges, tunnels and highways. Notably, such incidents could be staged in a way that would not even alert authorities to the onset of terrorist activity. In the New York metropolitan region in which Indian Point is sited, for example, a series of major accidents occurring at or about the same time would not be an unusual occurrence. In fact, on July 25, 2003, the very day the Federal Emergency Management Agency declared that the Indian Point emergency plan provided â€œadequateâ€• assurance of protection to the public, the entire New York metropolitan region was brought to a virtual traffic standstill after a tractor-trailer hit a beam on the George Washington Bridge and burst into flames, several minor accidents and a car fire took place on Interstate 95, and a truck got jammed under an overpass of the Hutchinson River Parkway. In 2006, a tanker truck carrying 8000 gallons of gasoline overturned on one of New York City's busiest highways, igniting a blaze that burned for hours and weakening the steel beams of an above bridge. Earlier this month a liquid propane explosion closed a 23 mile stretch of the New York State Thruway for hours, while firefighters had to stand by and watch the fire burn out because it was too hot to approach.

The staging of a couple of incidents like those just noted, combined with an â€œaccidentâ€• involving a tanker carrying hazardous gasses or liquids like liquefied ammonia, propane, chlorine, or vinyl chloride, prior to an assault would almost assuredly forestall the provision of outside assistance to a nuclear facility under attack.

## PLANTS MUST BE ABLE TO MOUNT A FULL DEFENSE WITHOUT RELIANCE ON OUTSIDE ASSISTANCE

Whether or not an attack employs strategies designed to obstruct regional transportation routes, numerous studies and the actual events of 9/11, Katrina, and Rita (as well as relatively minor events such as the January 18, 2006 wind storm in NY) demonstrate beyond cavil that first responder forces and the National Guard do not have the resources, manpower, equipment or communications capabilities to swiftly and adequately respond to a major assault on a nuclear facility. Just this very month, a report of the Commission on the National Guard and Reserves detailed the ongoing problem of inadequate human, equipment, communications and financial resources plaguing the National Guard. This report calls into question the ability of the government to bring all necessary assets to bear in the immediate aftermath of a major domestic incident.

In some regions - most notably the New York Metropolitan region, in which Indian Point is sited - roadway logistics and regular congestion alone would likely

prevent assisting forces from reaching a nuclear plant under attack in time. It bears mention that SWAT team assembly takes approximately 2 hours, whereas an assault could be over in a matter of minutes.

It is accordingly crucial that the NRC cedes the faulty assumption that plant personnel need only fend off attackers until law enforcement or military aid arrives. The fact that most regional first responders have little detailed knowledge of either the operational or internal layout of nuclear facilities further testifies to the folly of reliance upon the â€œcavalryâ€•.

ELEVATED VULNERABILITY TO INFILTRATION DURING EVENT

During a crisis event at a nuclear plant there also exists an elevated threat of infiltration by terrorists posing as first responders or National Guard. And in fact the imposter tactic has been used by terrorists in recent years with substantial success.

Terrorists disguised as firefighters could take particularly strong advantage of this stratagem. Outside firefighters often respond to fires at nuclear power plants and many attack scenarios would be expected to involve fire. Firefighters would presumptively be seen as benign by plant personnel and would have a legitimate reason to move throughout a facility and â€œcheckâ€• components such as electrical wiring. Moreover, bulky firefighter uniforms and equipment can hold and hide a host of articles that could be used for destructive purposes.

DEFENSE AGAINST A SIZABLE MULTI-TEAM, MULTI-DIRECTIONAL FORCE

In January 1991, the Nuclear Information Resource Service and the Committee to Bridge the Gap filed a joint Petition with the NRC requesting, inter alia, that the DBT be upgraded to 20 external attackers. The NRC rejected the petition in June 1991, asserting that an attack involving more than 3 assailants was unrealistic.

September 11 was a demonstration of the profound limitations of governmental foresight.

The September 11 plot involved 20 attackers (although only 19 were ultimately able to participate). The tragic 2004 siege at a school in Belsan, Russia involved more than 30 armed terrorists. It should be beyond question at this point that a terrorist attack could involve scores of attackers.

Accordingly, the PRSR must assume at least two dozen attackers. Lessons learned from 9/11 and the many multiple coordinated terrorist actions that have transpired in Europe, Asia and the Middle East since then, also mandate the premise that attackers will act in several teams and that some of those teams

may be sizable.

Any carefully planned attack on a nuclear facility by knowledgeable individuals, would also involve several different modus operandi. The PRSR should therefore take into account the consequences of near-simultaneous damage to different plant installations, systems and personnel (e.g., the effect of a small explosive-laden plane diving into the roof of a spent fuel pool coupled with the waterborne sabotage of the spent fuel pool intake system).

## A COORDINATED ATTACK ON MULTIPLE ON AND OFF-SITE TARGETS

A related point is that, following 9/11, the NRC can no longer ignore the very real possibility that an attack on a nuclear power plant would occur commensurate with an attack on other regional infrastructure such as chemical plants and bridges. A coordinated attack designed to effectively eradicate a region would very likely preliminarily target communication, electrical power and/or transportation infrastructures. This would ensure that (A) the targeted region is reduced to mass confusion, (B) local and federal officials and responders would be overwhelmed, and (C) law enforcement and other first responders would be impeded from gaining access to the nuclear plant site.

Certain areas of the U.S. offer a plethora of target opportunities and thus are particularly vulnerable to multiple target scenarios. Prime among them is the greater New York Metropolitan area (already in the terrorists' crosshairs) which contains numerous national landmarks, corporate headquarters, reservoirs, bridges, airports, transportation arteries and hazardous chemical plants, all in near vicinity to Indian Point, a mere 24 miles north of New York City.

## A CREDIBLE NUCLEAR PLANT SECURITY FORCE TESTING PROGRAM

The deficiencies, failures, and chicanery that have long plagued the various manifestations of nuclear power industry security drills and force-on-force (FOF) testing have been exhaustively documented in recent years. Noteworthy investigations in this regard have been conducted by the Project on Government Oversight (augmented by testimony provided in 2002 Senate Environment and Public Works Committee hearings) and the United States General Accounting Office (which reported its findings in a September 2003 report entitled â€œOversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthenedâ€•) as well as by the press. Problems with the FOF program are also addressed in the July 2004 Petition for Rulemaking to amend 10 CFR Part 73 to upgrade the DBT filed by the Committee to Bridge the Gap and the Comments on the DBT filed in 2006 by the Union of Concerned Scientists. CIECP fully endorses the recommendations made in previous filings by the Committee to Bridge the Gap and the Union of Concerned Scientists.

CIECP urges the NRC in the strongest possible terms to upgrade drills and

testing protocols to remedy the flaws that are a matter of public record and to take into account the realities noted herein. FOF tests must be sufficiently challenging to provide high confidence in the defensive capabilities of the security forces at the nation's 103 nuclear power plants. One clear failing of the FOF program to date has been the giving of excessive warning regarding upcoming tests. While some notice is necessary, one week should suffice. In addition, staff assignments should be frozen on the day of notice. This would eliminate the all too common practice of substituting a plant's most fit and accomplished security personnel in place of underachievers.

It is also critical that drills and the FOF program be revamped to eliminate manifest conflicts of interest. Examples of blatant conflicts of interest include: (1) The NRC allowing the nuclear industry's lobbying arm, the Nuclear Energy Institute (NEI) to award a FOF contract; and (2) The NEI, with NRC approval, then selecting Wackenhut, a corporation which contracts security guards to nuclear power plants in the U.S., to also be the contractor that supplies the mock adversary teams for the FOF tests.

Such problems have reduced the value of testing to the point where the FOF program lacks public confidence. The program must be redesigned and monitored by an independent entity such as the very capable U.S. military.

## HIGH TARGET APPEAL REACTORS

Prior terrorist attacks and plots against the U.S. have focused on major cities. It is a matter of fundamental logic that plants sited in highly populated metropolitan areas, particularly those with high symbolic value, face the greatest risk of being selected as a target.

It is thus imperative that the PRSR be modified to mandate a customized approach to high target nuclear facilities.

## SITE-SPECIFIC SAFETY-RELATED VULNERABILITIES

It is highly unrealistic to exclude from the PRSR calculus the reality of aging structures, deteriorated conditions and compromised systems that exist at various nuclear power plants in the U.S. A facility-customized approach must be taken which adds problems which are known or reasonably suspected and which could have a significant effect upon the ability of plant operators to maintain control during a major incident into the security equation.

Prime among factors which may be site-specific are:

o Corrosion and Embrittlement: For example, a risk of corrosion of the steel liner of the reactor containment at the Oyster Creek Nuclear Generating Station (Oyster Creek) was recently identified. A qualified corrosion expert

has warned that the risk may be high enough to cause buckling and collapse. Manifestly, corrosion or embrittlement-weakened structures and components are more vulnerable to the effects of heat and combustion.

o Vulnerability to Fire: Fire detection and suppression equipment and fire barriers are crucial to reactor safety. Over 20 years ago a worker at the Brown's Ferry Unit 1 reactor accidentally started a fire which destroyed emergency cooling systems and severely compromised the plant's ability to monitor its condition. In response, the NRC increased fire safety standards. In recent years, the NRC has effectively relaxed those standards. This is exceedingly unwise. During the chaos and threat level that would surely exist during a terrorist attack, human beings cannot be presumed to be able to take the actions necessary to protect critical systems from fire. The systems themselves must have integral safeguards. Yet plants such as Arkansas Nuclear One, Catawba, Ginna, H.B. Robinson, Indian Point, James A. Fitzpatrick, McGuire, Shearon Harris, Vermont Yankee and Waterford have been identified as having fire barrier wrap systems that failed fire tests. Fireproofing problems such as these jeopardize safe shutdown and must be recognized as a degradation of defense-in-depth protection. In addition, any plant fire hazard analyses must assume damage to multiple rooms and multiple structures, a circumstance that could easily result from an aircraft impact.

o Integrity of Structures that Support Mobility: While the focus of NRC regulatory review is on structures and equipment directly related to safe operational function, the conditions that may prevail during an assault would likely require plant personnel to be able to move rapidly throughout the facility. The evaluation of the reliability of structural features such as stairways (which might buckle or melt during a fire) is accordingly critical.

o Electrical System Problems: In 2003, a cable failure knocked out power to approximately half the safety systems at Oyster Creek, including security cameras, alarms, sensors, pumps and valves. In February 2003, all 4 of the backup generators at Fermi became simultaneously inoperable. In December 2001, Indian Point reactor 2 lost power due to a malfunction of the turbine, then lost back-up power to the reactor coolant system because of a second electrical failure. During the August 2003 blackout that struck the Northeast, following the loss of off-site power, two of Indian Point's emergency backup generators (both of which had been previously flagged as having problems) failed to operate. In view of the severe consequences failures such as these could have were they to occur during a major incident, known plant electrical system vulnerabilities must be taken into consideration.

o Cooling System Problems: Cooling system problems and design deficiencies have plagued a number of plants in recent years. In some cases the NRC has allowed plants to operate for long periods with compromised emergency cooling systems. For example, the Salem nuclear power station had experienced two years of repeated malfunctions of its high-pressure coolant-injection system prior to the time, in October 2003, when operators unsuccessfully tried to use it to

387

stabilize water levels following a steam pipe burst. And the NRC has allowed reactors with emergency sump pumps flagged as likely to become clogged and inoperative to remain in operation for many years without repair. The Los Alamos National Laboratory, for instance, concluded that the sump pumps at Indian Point reactors 2 and 3 could become clogged in as little as 23 minutes and 14 minutes, respectively. While, upgrades are being made, the failure of the NRC to mandate immediate correction of cooling system vulnerabilities calls its oversight capabilities seriously into question. Indeed the functional declination of critical systems must be deemed a constituent element of site-specific PRSR analyses.

## ELIMINATE COMMERCIAL CONSIDERATIONS FROM THE PRSR CALCULUS

The commercial interests of the nuclear industry are of valid concern to nuclear utilities and the NEI; they should not be of concern to the NRC. There is no justification for jeopardizing national security and the health and safety of the public - even to the smallest degree - to safeguard corporate profits.

The NRC has stated that its promulgated security standards are based upon the analysis of the largest threat against which a â€œprivate security force could reasonably be expected to defendâ€• [emphasis added] 70 FR 67385.

Both the NRC and the industry have acknowledged that, in their estimation, a private guard force should not be reasonably expected to defend against a 9/11-type attack involving aircraft. Such an attack, apparently, is deemed to fall under the loophole of 10 CFR Sec. 50.13, which exempts reactor operators from defending against â€œan enemy of the United States, a foreign government or other personâ€•. The perimeter of this â€œenemy of the United States provision has never been defined, so there is no way to know how far it extends. However, it is abundantly clear from the public record that the NRC has drawn the line at point where the profit margins of nuclear power operators might be significantly affected. Unfortunately, the terrorists are constrained by no such boundary.

Congress has charged the NRC with the obligation to protect the public health and safety. This must not be viewed simply as a guideline; it must be viewed as an uncompromised mandate.

If the NRC does not believe its licensees can afford the security upgrades necessary to protect the nation's nuclear reactors against the full potential threat, it must act with forthrightness and publicly demand that the Department of Homeland Security or the U.S. military assume responsibility for domestic nuclear power plant security.

## CONCLUSION

The 9/11 Commission observed: â€œAcross the government, there were failures of

imagination, policy, capabilitiesâ€¦The most important failure was one of imagination. We do not believe leaders understood the gravity of the threat.â€•

388

As a public interest group we ask: What needs to happen before the gravity of the threat is not only understood, but acted upon?

Respectfully submitted,

COUNCIL ON INTELLIGENT ENERGY
& CONSERVATION POLICY
(New York)
By

Michel C. Lee, Esq.
Chairman

(914) 393-2930

APPENDIX A

Since September 11, 2001, there has been much speculation about the vulnerability of nuclear power plants to aerial attack. Certainty, however, is in short supply.

What is known is that none of the nuclear reactors presently operational in the United States were built to withstand the crash of a jumbo jet, much less the crash of super jumbo such as the A380 which will take to the air weighing 1.2 million pounds, has a wingspan almost as long as a football field, is 8 stories tall, and is 3 times as large as the 767s that brought down the Twin Towers.

Nevertheless studies that have addressed the prospect of planes hitting nuclear plants include the following:

1974: To date the only published peer reviewed study on the vulnerability of U.S. nuclear power plants was conducted by General Electric, the leading builder of nuclear plants, and published in the industry journal Nuclear Safety. GE looked at accidents -not terror attacks - and concluded that were a â€œheavyâ€• airliner to hit a reactor building in the right place, it would almost certainly rip it apart. Such a hit would also most likely damage the reactor core and both the cooling and emergency cooling systems. [NOTE: The GE study defined a â€œheavyâ€• plane as one weighing more than 6 tons. The Boeing 757 which gouged a 100 foot gash through the reinforced concrete of the Pentagon weighed between 80

and 100 tons. A fully loaded 767 weighs over 200 tons. The Airbus 380, expected to be launched into commercial use later this year, takes to the air weighing 1.2 million pounds, hundreds of thousands of pounds heavier than the Boeing 747, the current jumbo of the sky.]

1982: A technical report (previously publicly available) of a study conducted by the U.S. Army Corps of Engineers at the NRC's behest focused on plane crash analyses at the Argonne National Laboratory. The Corps concluded that planes traveling at a speed of over 466 mph would crash through the average reactor containment structure noting â€œaccount has been taken of the internal concrete wall which acts as a missile barrierâ€¦It would appear, however, that this is too optimistic since vaporized fuel, hot gaseous reaction products, and to a certain extent portions of liquid fuel streams will flow around such obstructions and overwhelm internal defensesâ€¦.â€• [NOTE: An FBI analysis estimated that American Airlines Flight 11, which hit the north tower of the World Trade Center, was traveling at a speed of 494 mph, and that United Airlines Flight 175, which hit the south tower, was traveling at 586 mph, a speed far exceeding its design limit for the altitude.]

2000: A NRC study published less than a year before September 11 calculated that 1 out 2 commercial airplanes flying in the year 2000 were large enough to penetrate even a 5 foot thick reinforced concrete wall 45% of the time. Specifically, the study states, â€œaircraft damage can affect the structural integrity of the spent fuel pool or the availability of nearby support systems, such as power supplies, heat exchangers, or water makeup sources and may also affect recovery actionsâ€¦It is estimated that half the commercial aircraft now flying are large enough to penetrate the 5 foot thick reinforced concrete walls.â€• [NOTE: The thickness of the top of certain reactor domes is 3 and-a-half feet.]

2002: The German Reactor Safety Organization (GRS) a scientific-technical research group that works primarily for nuclear regulators in Germany conducted an extremely detailed study that determined that terrorists can, with a strategically targeted airplane crash, initiate a nuclear accident. (A secret Ministry document that summarized the report was leaked to the German and Austrian press and subsequently translated into English.) The GRS study used dynamic computation modeling that looked at the potential consequences of a wide range of impact possibilities on different plant equipment and installations. Different types of airplanes, velocities, angles of impact, weight loads and fuel effects were considered, as were various sequences of events. Aside from the basic finding of vulnerability, the GRS study is significant for recognizing the limitations of even its highly complex analyses. Key unknowns include the impacts of fire loads on many kind of materials and equipment as well as the behaviors of various combustive materials under the conditions of a plane crash.

2004: In 2004 the U.K. Parliamentary Office of Science and Technology (OST) issued a secret report on the risks of terrorist attacks on nuclear facilities

390

to the U.K. House of Commons Defense Committee. The OST report was leaked to the magazine New Scientist, which reported the OST conclusion that a large plane crash into a nuclear reactor could release as much radiation as the1986 accident at Chernobyl, while a crash into the nuclear waste tanks at the U.K.'s Sellafield facility could cause several million fatalities.

From these studies it is clear that there exists a reasonable basis for concern regarding malevolent deployment of aircraft against nuclear power facilities.

It should also be evident that all studies on this topic are, in substance, educated conjecture. The current state of computer modeling is not up to analyzing the full range of physical and chemical interactions that could occur under the incalculable range of different kinds of aircraft, approaching at different angles, at different speeds, hitting different structures, which all have facility-unique room and equipment layouts, and different substance, chemical, and ventilation-related conditions.

A lesson in the unpredictable consequences of airplane crashes was brought home on September 11 (when even the 47 story tall 7 World Trade Center that was not struck collapsed for reasons engineers have yet to fully determine). A lesson in the limitations of advanced computer modeling can also be learned from the Columbia space shuttle disaster.

[~DBT and PRSR]

**********

Nuclear Power Plants: Vulnerability to Terrorist AttackThis is the
html version of the file
http://vienna.usembassy.gov/en/download/pdf/nucl_plants_attacks.pdf.
G o o g l e automatically generates html versions of documents as we
crawl the web.
To link to or bookmark this page, use the following url:
http://www.google.com/search?q=cache:Qu_4R9wicMQJ:vienna.usembassy.gov/en/download/pdf/nucl_plants_attacks.pdf+by+Carl+Behrens+and+Mark+Holt,+Nuclear+Power+Plants:+Vulnerability+to+Terrorist+Attack&hl=en&ct=clnk&cd=1&gl=us


These search terms have been highlighted: carl behrens mark
holt nuclear power plants vulnerability terrorist attack

Page 1
Congressional Research Service Ëœ The Library of CongressCRS Report for
CongressReceived through the CRS WebOrder Code RS21131Updated August 9,
2005Nuclear Power Plants: Vulnerability to Terrorist AttackCarl Behrens and Mark
HoltSpecialists in Energy PolicyResources, Science, and Industry
DivisionSummaryProtection of nuclear power plants from land-based assaults,
deliberate aircraftcrashes, and other terrorist acts has been a heightened
national prioritysince the attacksof September 11, 2001. The Nuclear Regulatory
Commission (NRC) has strengthenedits regulations on nuclear reactor security,
butcritics contend that implementation bytheindustry has been too slow and that
further measures are needed. Several provisions toincrease nuclear reactor
security are included in the Energy Policy Act of 2005, signedAugust 8, 2005.
The new law requires NRC to conduct â€œforce on forceâ€• securityexercises at
nuclear power plants at least once every three years and to revise
theâ€œdesign-basis threatâ€• that nuclear plant security forces must be able to
meet, amongother measures. This report will be updated as events warrant.Nuclear
power plants have long been recognized as potential targets of terroristattacks,
and critics havelongquestioned theadequacyof themeasuresrequired of nuclearplant
operators to defend against such attacks. Followingthe September 11, 2001,
attackson the Pentagon and the World Trade Center, the Nuclear
RegulatoryCommission (NRC)began a â€œtop-to-bottomâ€• review of its security
requirements. On February 25, 2002, theagency issued â€œinterim compensatory
security measuresâ€• to deal with the â€œgeneralizedhigh-level threat environmentâ€•
that continued to exist, and on January 7, 2003, it issuedregulatory orders that
tightened nuclear plant access. On April 29, 2003, NRC issuedthree orders to
restrict security officer work hours, establish new security force trainingand
qualification requirements, and increase the â€œdesign basis threatâ€• thatnuclear
securityforces must be able to defeat.Security RegulationsUnder the regulations
in place prior to the September 11 attacks, all commercialnuclear power plants
licensed by NRC must be protected by a series of physical barriersand a trained
security force. The plant sites are divided into three zones: an
â€œowner-controlledâ€• buffer region, a â€œprotected area,â€• and a â€œvital area.â€• Access
to the protectedarea is restricted to a portion of plant employees and monitored
visitors, with stringent

Page 2
CRS-21General NRC requirements for nuclear power plant security can be found at
10 CFR 73.55.2Government AccountabilityOffice. NuclearRegulatoryCommission:
Preliminary Observationson Efforts to Improve Security at Nuclear Power Plants.
Statement of Jim Wells, Director,Natural Resources and Environment, Government
Accountability Office, to the Subcommitteeon National Security, Emerging
Threats, and International Relations, House Committee onGovernment Reform.
September 14, 2004. p. 14.access barriers. The vital area is further restricted,
with additional barriers and accessrequirements. The security force must comply
with NRC requirements on pre-hiringinvestigations and training.1Design Basis
Threat. The severity of attacks to be prepared for are specified inthe form of a
â€œdesign basis threatâ€• (DBT). One of NRCâ€™s April 2003 regulatory orderschanged

291

the DBT to â€œrepresent the largest reasonable threat against which a regulatedprivate guard force should be expected to defend under existing law,â€• according to theNRC announcement. The details of the revised DBT, which took effect October 29, 2004,were not released to the public.NRC requires each nuclear power plant to conduct periodic securityexercises to testits ability to defend against the design basis threat. In these â€œforce on forceâ€• exercises,monitored by NRC, an adversary force from outside the plant attempts to penetrate theplantâ€™s vital area and damageordestroykeysafetycomponents. Participants in the tightlycontrolled exercises carry weapons modified to fire only blanks and laser bursts tosimulate bullets, and they wear laser sensors to indicate hits. Other weapons andexplosives, as well as destruction or breaching of physical security barriers, may also besimulated. While one squad of the plantâ€™s guard force is participating in a force-on-forceexercise, another squad is also on dutyto maintain normal plant security. Plant defendersknow that a mock attack will take place sometime during a specific period of severalhours, but they do not know what the attack scenario will be. Multiple attack scenariosare conducted over several days of exercises.Full implementation of theforce-on-forceprogram coincided with theeffectivedateof the new DBT in late 2004. Standard procedures and other requirements have beendeveloped for using the force-on-force exercises to evaluate plant security and as a basisfor taking regulatory enforcement action. Many tradeoffs are necessary to make theexercises as realistic and consistent as possible without endangering participants orregular plant operations and security. Each plant is required to conduct NRC-monitoredforce-on-force exercises once every three years.NRC required the nuclear industry to develop and train a â€œcomposite adversaryforceâ€• comprising security officers from many plants to simulate terrorist attacks in theforce-on-force exercises. However, in September 2004 testimony, the GovernmentAccountabilityOffice (GAO) criticized the industryâ€™sselectionof a securitycompanythatguards about half of U.S. nuclear plants, Wackenhut, to also provide the adversaryforce.In addition to raising â€œquestions about the forceâ€™s independence,â€• GAO noted thatWackenhut had been accused of cheating on previous force-on-force exercises by theDepartment of Energy.2

Page 3

CRS-3Congress imposed statutoryrequirements for the DBT and force-on-force exercisesin the Energy Policy Act of 2005, signed August 8, 2005. The act requires that eachnuclear plant undergo force-on-force exercises at least once every three years (NRCâ€™scurrent policy), thattheexercises simulatethethreats in theDBT, and thatNRC â€œmitigateany potential conflict of interest that could influence the results of a force-on-forceexercise, as the Commission determines to be necessary and appropriate.â€•The new law requires NRC to revise the DBT within 18 months, after consideringa wide variety of potential modes of attack (physical, chemical, biological, etc.), thepotential for large attacks by multiple teams, potential assistance by several employeesinside a facility, the effects of large explosives and other modern weaponry, and otherspecific factors.Emergency Response. After the 1979 accident at the Three Mile Island nuclearplant near Harrisburg, PA, Congress required that all nuclear power plants be covered byemergency plans. NRC requires that within an approximately 10-mile EmergencyPlanning Zone (EPZ) around each plant the operator must maintain warning sirens andregularly conduct evacuation exercises monitored by NRC and the Federal EmergencyManagement Agency (FEMA). In light of the increased possibility of terrorist attacksthat, if successful, could result in release of radioactive material, critics have renewedcalls for expanding the EPZ to include larger population centers.Another controversial issue regarding emergency response to a radioactive releasefrom a nuclear power plant is the distribution of iodine pills. A significant component ofan accidental or terrorist release from a nuclear reactor would be a radioactive form ofiodine, which tends to concentrate in the thyroid gland of persons exposed to it. Takinga pill containing non-radioactive iodine before exposure would prevent absorption of theradioactive iodine. Emergency plans in many states include distribution of iodine pillsto the population within the EPZ, which would protect from exposure to radioactiveiodine, although giving no protection against other radioactive elements in the release.NRC in 2002 began providingiodine pills to states requestingthem for populations withinthe 10-mile EPZ.Nuclear Plant VulnerabilityOperating nuclear reactors contain large amounts of radioactive fission productswhich, if dispersed, could pose a direct radiation hazard,



٢٤٤

contaminate soil and vegetation,and be ingested by humans and animals. Human exposure at high enough levels cancause both short-term illness and death, and longer-term deaths by cancer and otherdiseases.To prevent dispersal of radioactive material, nuclear fuel and its fission products areencased in metal cladding within a steel reactor vessel, which is inside a concreteâ€œcontainmentâ€• structure. Heat from the radioactive decay of fission products could meltthe fuel-rod cladding even if the reactor were shut down. A major concern in operatinga nuclear power plant, in addition to controlling the nuclear reaction, is assuring that thecore does not lose its coolant and â€œmelt downâ€• from the heat produced bythe radioactivefission products within the fuel rods. Therefore, even if plant operators shut down thereactor as they are supposed to during a terrorist attack, the threat of a radioactive releasewould not be eliminated.

Page 4

CRS-43Letter from NRC Chairman Nils J. Diaz to Secretary of Homeland Security Tom Ridge,September 8, 2004.Commercial reactor containment structures â€" made of steel-reinforced concreteseveral feet thick â€" are designed to prevent dispersal of most of a reactorâ€™s radioactivematerial in the event of a loss of coolant and meltdown. Without a breach in thecontainment, and without some source of dispersal energy such as a chemical explosionor fire, the radioactive fission products that escaped from the meltingfuel claddingmostlywould remain where theywere. The two major meltdown accidents thathave taken placein power reactors, at Three Mile Island in 1979 and at Chernobyl in the Soviet Union in1986, illustrate this phenomenon. Both resulted from a combination of operator error anddesign flaws. At Three Mile Island, loss of coolant caused the fuel to melt, but there wasno fire or explosion, and the containment prevented the escape of substantial amounts ofradioactivity. At Chernobyl, which had no containment, a hydrogen explosion and afierce graphite fire caused a significant part of the radioactive core to be blown into theatmosphere, where it contaminated large areas of the surrounding countryside and wasdetected in smaller amounts literally around the world.Vulnerabilityfrom Air Attack. Nuclear power plantswere designed towithstandhurricanes, earthquakes, and other extreme events, but attacks by large airliners loadedwith fuel, such as those that crashed into the World Trade Center and Pentagon, were notcontemplated when design requirements were determined. A taped interview shownSeptember 10, 2002, on Arab TV station al-Jazeera, which contains a statement that AlQaeda initially planned to include a nuclear plant in its 2001 attack sites, intensifiedconcern about aircraft crashes.In light of the possibilitythat an air attack might penetrate the containment buildingof a nuclear plant, some interest groups have suggested that such an event could befollowed by a meltdown and widespread radiation exposure. Nuclear industryspokespersons have countered by pointing out that relatively small, low-lying nuclearpower plants are difficult targets for attack, and have argued that penetration of thecontainment is unlikely, and that even if such penetration occurred it probablywould notreach the reactor vessel. Theysuggest that a sustained fire, such as that which melted thestructures in the World Trade Center buildings, would be impossible unless an attackingplane penetrated the containment completely, including its fuel-bearing wings.Recentlycompleted NRC studies â€œconfirm that the likelihood of both damaging thereactor core and releasing radioactivity that could affect public health and safetyis low,â€•according to NRC Chairman Nils Diaz. However, NRC is considering studies ofadditional measures to mitigate the effects of an aircraft crash.3Spent Fuel Storage. Radioactive â€œspentâ€• nuclear fuel â€" which is removed fromthe reactor core after it can no longer efficiently sustain a nuclear chain reaction â€" isstored in pools of water in the reactor building or in dry casks elsewhere on the plantgrounds. Because both types of storage are located outside the reactor containmentstructure, particular concern has been raised about the vulnerabilityof spent fuel to attackby aircraft or other means. Spent fuel pools and dry cask storage facilities are subject toNRC security requirements.

Page 5

CRS-54National Academy of Sciences, Board on Radioactive Waste Management, Safety and Securityof Commercial Spent Nuclear Fuel Storage, Public Report (online version), released April 6,2005.510 CFR 73.55 (h)(3) states: â€œThe total number of guards, and armed, trained personnelimmediately available at the facility to fulfill these response requirements shall nominally be ten(10), unless specificallyrequired otherwise on a case bycase basis bythe Commission;



343

however,this number may not be reduced to less than five (5) guards.â€•The primary concern is whether terrorists could breach the thick concrete walls ofa spent fuel pool and drain the cooling water, which could cause the spent fuelâ€™szirconium cladding to overheat and catch fire. A report released in April 2005 by theNational Academy of Sciences (NAS) found that â€œsuccessful terrorist attacks on spentfuel pools, though difficult, are possible,â€• and that â€œif an attack leads to a propagatingzirconium cladding fire, it could result in the release of large amounts of radioactivematerial.â€• NAS recommended thatthehottest spent fuelbeinterspersedwith coolerspentfuel to reduce the likelihood of fire, and that water-spray systems be installed to coolspent fuel if pool water were lost. The report also called for NRC to conduct moreanalysis of the issue and consider earlier movement of spent fuel from pools into drystorage.4Both the House- and Senate-passed versions of the FY2006 Energy and WaterDevelopment appropriations bill (H.R. 2419, H.Rept. 109-86, S.Rept. 109-84) wouldprovide $21 million for NRC to carry out the NAS recommendations. The HouseAppropriationsCommitteewas particularlycriticalof NRCâ€™s actions on spent fuelstoragesecurity: â€œThe Committee expects the NRC to redouble its efforts to address the NAS-identified deficiencies, and to direct, not request, industry to take prompt correctiveactions.â€•Regulatory and Legislative ProposalsCritics of NRCâ€™s security measures have demanded both short-term regulatorychanges and legislative reforms.A fundamental concern was the nature of the DBT, which critics contended shouldbeincreased to include a number of separate, coordinated attacks. Critics also contendedthat nearlyhalf of the plants tested in NRC-monitored mock attacks before 9/11 failed torepel even the small forces specified in the original DBT, a charge that industry sourcesvigorously denied. Critics also pointed out that licensees are required to employ only aminimum of five securitypersonnel on dutyper plant, which theyargue is not enough forthe job.5Nuclear spokespersons responded that the actual security force for the nationâ€™s65 nuclear plant sites numbers more than 5,000, an average of about 75 per site (coveringmultiple shifts). Nuclear plant security forces are also supposed to be aided by local lawenforcement officers if an attack occurs.In February2002, NRC implemented what it called â€œinterim compensatorysecuritymeasures,â€• including requirements for increased patrols, augmented security forces andcapabilities, additional securityposts, installation of additional physical barriers, vehiclechecks at greater stand-off distances, enhanced coordination with law enforcement andmilitaryauthorities, and more restrictive site access controls for all personnel. The further

orders issued April 29, 2003, expanded on the earlier measures, including revising theDBT, which critics continue to describe as inadequate. Continuing congressionalconcerns resulted in the new criteria in the Energy Policy Act of 2005 for further DBTrevisions.Because of the growingemphasis on security, NRCestablished the Office of NuclearSecurity and Incident Response on April 7, 2002. The office centralizes securityoversight of all NRC-regulated facilities, coordinates with law enforcement andintelligence agencies, and handles emergency planning activities. Force-on-forceexercises are an example of the officeâ€™s responsibilities. On June 17, 2003, NRCestablished the position of Deputy Executive Director for Homeland Protection andPreparedness, whose purview includes the Office of Nuclear Security and IncidentResponse.Legislation. Since the 9/11 attacks, numerous legislative proposals, includingsome by NRC, have focused on nuclear power plant security issues. Several of thoseideas, such as the revision of the design-basis threat and the force-on-force securityexercises, were included in the Energy Policy Act of 2005, which also includes:!assignment of a federal security coordinator for each NRC region;!backup power for nuclear plant emergency warning systems;!tracking of radiation sources;!fingerprinting and background checks for nuclear facility workers;!authorizing use of firearms by nuclear facility security personnel(preempting some state restrictions);!authorizing NRC to regulate dangerous weapons at licensed facilities;!extending penalties for sabotage to cover nuclear facilities underconstruction;!requiring a manifest and personnel background checks for import andexport of nuclear materials; and!requiring NRC to consult with the Department of Homeland Securityonthe vulnerability to terrorist attack of locations of proposed nuclearfacilities before issuing a license. A number of legislative proposals introduced since 9/11 to increase nuclear plantsecuritywere not included in the new law, including the creation of



374

a federal force withinthe NRC to replace the private guards at nuclear power plants, requiring emergencyplanning exercises within a 50-mile radius around each nuclear plant, and stockpilingiodine pills for populations within 200 miles of nuclear plants. Other measures proposedbut not enacted include a task force to review security at U.S. nuclear power plants anda federal team to coordinate protection of air, water, and ground access to nuclear powerplants.



55