7.18 BACKUP CONTROL SYSTEM

7.18.1 Design Objectives

The design objective of the Backup Control System is to provide: (1) a means to safely shut down the plant from locations outside the main control rooms, contiguous rooms at the same level as the control rooms, the spreading rooms, and contiguous rooms below the spreading rooms, collectively referred to as the control bay, and (2) a sufficient complement of suitable instrumentation and controls to bring the plant to the cold condition in an orderly fashion and maintain it in that state indefinitely.

Detailed requirements for achieving a safe and stable condition following a fire in the control room and evacuation of the control room are provided in the Fire Protection Report.

7.18.2 Design Bases

The Backup Control System shall be designed to:

a. Provide for safe shutdown of any or all of the units in the plant after gross damage to the Control Bay (i.e., main control rooms, contiguous rooms at the same level as the control rooms, the spreading rooms and contiguous rooms in the level below the spreading rooms).

b. Provide redundant or diverse controls over the methods for cooling the reactors and removing heat dissipated to the containments.

c. Perform its function without creating any new common points of vulnerability in the control bay.

d. Perform its function without obtaining information from any sources in the control bay which may be damaged, inaccessible, etc..

e. Prevent failure in or to the backup control information readout equipment indicators from influencing the redundant readout equipment in the control room.

f. Maintain the separations of the divisions of backup control outside the control bay such that no failure will deprive the plant of essential shutdown services.

g. Consistent with (c) above, transfer control from the control room to the backup control locations regardless of the condition of the circuits in the control room (e.g., shorts, open-circuits, or grounds).

h. Provide control room annunciation of any transfer switch that is turned from its normal position.

i. Provide only shutdown capability from a normal operating state without consideration of any other accidents, such as LOCA, prior to or after the event that damages the control room.

j. Shut the plant down to essentially the same state as would occur with a loss of offsite power without incremental fuel failures.

k. Correct any spurious opening of valves which would lead to a loss of coolant or admission of high pressure fluids to low pressure systems.

l. Provide for manual operation of valves for only essential services, such as main steam, RBCCW, RHR, EECW, ADS inhibit, selected MSRVs, etc. (The general function of containment isolation is not required to be operable.)

m. Provide environmental protection at the backup control locations for operators and equipment regardless of the conditions in the control room.

n. Provide for initiating and maintaining backup control with the reactors at any normal operating pressure and level.

o. Provide for implementing of backup control with onsite power automatically available upon loss of offsite power; however, manual controls of the diesel generators shall be available as a backup for automatic transfer on loss of offsite power.

p. Provide for remote load control (4KV Shutdown Boards) to replace the electrical control board in the main control room. Alarms may be monitored from the diesel information panel for Unit 1/2 and from the 4KV Shutdown Boards for Unit 3..

q. Have redundant communication system(s) available between the backup control centers: electrical board rooms (includes shutdown board rooms), the Diesel Generator Buildings, the RCIC Relay Panels, and any other necessary locations.

r. Provide for operation of the fire pumps directly from the 4160-V shutdown boards irrespective of the condition of the control room.

7.18.3 Description

The Backup Control System is a variation of the normal system used inside the control room to shut down the reactor when normal feedwater and electrical control

power supplies are not available and the normal heat sinks (turbines and condensers) may not be available. Reactor pressure is controlled and reduced, while decay heat and sensible heat are removed, by dumping steam through the main steam relief valves to the pressure suppression pool. The reactor pressure boundary is protected by the backup controls so that spurious openings of valves which could cause a loss of coolant or admit high pressure to low pressure piping systems are prevented.

Reactor water inventory is maintained by RCIC while the reactor(s) are above 50 psig (RCIC operates at a reduced flow rate between 50 psig and 150 psig reactor pressure) and augmented as desired (but not necessarily) by the control rod drive pumps while the reactor(s) are above 50 psig. Below 150 psig, makeup water can also be supplied from the RHR System as well as from control rod drive pumps, the RHRSW pumps or the condensate pumps, the pressure suppression pool is cooled by circulating the principal flow through the RHR pumps into and through the torus via the test bypass. These valves are designed for throttling.

All RHR pumps, all RHRSW pumps, and two heat exchangers per unit are equipped with backup controls to provide redundancy. On a three-unit basis, only one RHR pump, one RHR heat exchanger, and one RHRSW pump (providing cooling water to the heat exchanger) are necessary to be concurrently operated per unit for reactor and suppression pool cooling. Two of the RHRSW pumps are operated to provide cooling water to the EECW System via both header systems. The EECW System is provided with backup controls to ensure redundant operation of this system as an entity.

The onsite diesel generator system and associated shutdown boards are available to the Backup Control System. Load control for the Unit 1/2 and/or Unit 3 diesels may be directed from their respective remote locations (Diesel Information Center and 4KV Shutdown Boards for Unit 1/2 and 4KV Shutdown Boards for Unit 3). Actual load manipulations are carried out at the 4KV Shutdown Boards in their respective electrical board rooms. Essential plant parameters are monitored from the backup control panels located in the electrical board rooms.

Undesired loads which might occur from circuit malfunctions are prevented by manual switching at the boards. All board breakers (except transformer breakers) are provided with transfer switches on the front of the individual panels at the equipment locations. These transfer switches are two-position "Normal-Emergency"

switches which, when in "Emergency" mode, preclude spurious breaker operations from remote or automatic sources as required.

7.18.4 System Operation

The Backup Control System is put in operation when the control room operators are forced to evacuate. They would proceed to various locations in the diesel building, control building, and reactor building to shutdown board rooms, electrical board rooms, etc., which are provided with suitable instrumentation and controls from which they can effect and maintain a safe shutdown condition for an indefinitely long time. The detailed procedures for implementing backup controls will rely on the Shift Manager to initiate emergency action. Initially, the Shift Manager makes an assessment of the situation and attempts corrective measures to preclude evacuation. If abandonment becomes necessary, operators will scram the reactor by the scram switches at the Main Control Room panel, trip the recirculation pumps, start the onsite power system, and the EECW System (2 pumps). The main turbine is tripped and bypass operation is continued for as long as possible. The operators are dispatched to the dispersed backup control centers in the shutdown board rooms. The operators perform at the backup control centers and operate the transfer switches to disconnect the main steam relief valves (this prevents spurious blowdown of the primary system), and then operate the transfer switches on the main steam line isolation valves to transfer control to the Backup Control System. All other transfers are accomplished by special switches at the switchgear and/or the motor control centers, and/or remote locations, except some of those for RCIC are done at the RCIC relay panel in the Reactor Building near the backup control center. After operation of all the transfer switches, the plant is then shut down in an orderly manner to the cold condition.

7.18.5 Design Evaluation

The Backup Control System is not an engineered safety feature, but is a design feature to cope with a forced evacuation from the control room(s). Fires or some other gross event could cause a forced evacuation of the Main Control Room, as well as cause common damage and loss of the control circuits multiple divisions of protection, safeguards equipment, and auxiliary supporting systems. Primarily, because of loss of control of the latter group of systems, the consequences of such an incident could be that the operating condition of the affected units might degrade to an indeterminate and/or unsafe state. This Backup Control System is designed to prevent this degradation, irrespective of the condition of the control and spreading rooms, and the circuits and equipment therein, and thus, provide for the capability to safely shut down the plant from outside the control room(s). (However, the event which occurred to cause such damage is considered to be a major damaging event in its own right, and is not an event preceding or following a loss-of-coolant accident.)

In effect, the system provides protection against damage in the control bay and is physically and electrically separated from these damaged areas. The system provides redundancy or a diverse means to effect a cold shutdown (MODE 4) condition considering the single failure criterion.

The transfer switches are of the maintained contact type, and transfer of any switch to the emergency position is annunciated in the Main Control Room.

The addition of the Backup Control System does not introduce any new common points of vulnerability, nor does it create any significant new hazards to existing safety circuits. Thus, the plant will not endanger the health and safety of the public under the condition of forced evacuation of the control room, even if unspecified damage occurs in the control room or the control bay.

7.18.6 Inspection and Test

Any malpositioned transfer switches can be detected during operation and immediate corrective measures will be taken. Operability of components from the Backup Control Center will be tested to the extent practical once per operating cycle. This includes testing of transfer of control of active components and instrument calibration.