JUL 15 1970

OCONEE NUCLEAR STATION

DOCKET NOS. 50-269, -270 AND -287

SAFETY EVALUATION

PROTECTION SYSTEM

General

The design of the protection system, which consists of the reactor trip system and the engineered safety feature actuation system, is identical for all three Oconee units. Each unit's protection system is completely independent except for the shared 125 Vdc instrument power system which is discussed later in this report. Our review included a detailed study of the schematic diagrams of the reactor trip system and the actuation circuitry of the engineered safety feature systems.

Conformance of the protection system to the Commission's proposed General Design Criteria (GDC), as published in the Federal Register on July 11, 1967, and the Proposed IEEE Criteria for Nuclear Power Plant Protection Systems (IEEE 279) dated August, 1968, served, where applicable, as the principal basis for our conclusion that the protection system is, except as discussed later in this report, acceptable.

Reactor Protection System

The reactor protection system consists of four identical channels, each of which utilizes general logic and de-energizes (trips) upon detection of any one of the conditions listed in Table 7-1 of the FSAR. Each channel terminates in a reactor trip module which controls one or more breakers in the control rod drive power system. The system logic is 2/4, i.e., if any two protection channels trip, all reactor trip modules trip commanding all control rod breakers to trip. The entire system, from the process sensors to the control rod breakers, is testable during reactor operation.

a. Bypassing

Section 7.1.2.3.8 of the FSAR discusses the three means by which various reactor trip signals can be bypassed. Based on our review, we conclude that administrative controls provide the only significant protection against improper use of these bypasses. Our evaluation of each of the three bypass provisions is discussed below:

1. Channel Bypass Switches: Section 4.11 of IEEE 279 permits one channel to be bypassed during reactor operation but positive means of ensuring that the remaining

portion of the protection system continues to meet the single failure criterion are not specifically required. Although it is possible to completely bypass the automatic portion of the reactor trip system, we conclude that administrative control of the number of channel bypass switch keys (one per reactor unit) and of the number of channels bypassed concurrently (one per reactor unit), together with indication of the channel which is bypassed, meets the intent of IEEE 279 and is acceptable. The Technical Specification will require that no more than one trip channel be bypassed concurrently.

2. Shutdown Bypass Switches: Although a pressure interlock prevents use of these switches during power operation, the applicant has stated that, in order to provide adequate protection during physics testing and control rod drive testing, the high power level trip set points must be lowered. The applicant proposes to change the set points manually. We have not completed our review of this portion of the design. Our conclusions regarding the acceptability of the manual set point adjustments will be forwarded to the Committee in a supplemental report on the Oconee facility in August, 1970.

3. Dummy Bistables: Dummy bistables, which bypass the individual input signals, can be installed in each reactor trip channel. As presently proposed, no indication is provided to indicate either the number of dummy bistables installed or the instrument channel in which they are installed. Although we are unable to report our final position on the use of the dummy bistables, there are only three alternatives presently under consideration: (1) If the design is not changed, we would not permit the use of dummy bistables; (2) The applicant has stated that the design could be easily changed to provide indication of the trip channel, but not the instrument channel, in which dummy bistables are installed. If this design change is made, the use of dummy bistables in one trip channel at a time would meet IEEE 279. Concurrent use of a channel bypass switch and dummy bistables would not meet IEEE 279; (3) If the design is changed to meet our interpretation of IEEE 279, i.e., the status of the protection system is continuously, and in a non-ambiguous manner, indicated to the operator, we could permit the use of dummy bistables within the Technical Specification requirements for a minimum of two operable instrument channels per trip parameter with the trip channels arranged in a one-out-of-two trip logic.

b. Operation With Less Than Four Reactor Coolant Pumps

The design of the reactor protection system includes provisions for operation with less than four reactor coolant pumps in service. Operation with three pumps running requires no adjustment of protection system set points because the power/flow trip can provide adequate protection. An automatic set point change is made when only one pump in each loop is in operation; this set point change limits reactor operation to less than 55% of rated power. Loss of two pumps in the same loop will cause a reactor trip regardless of power level. In order to resume operation with only the other two pumps in service, the applicant proposes to manually change several protection system set points. Operation with only one pump in service is not proposed. We conclude that this design is acceptable for the Oconee units for the following reasons:

1. Operation with less than four coolant pumps running is not a planned mode of operation unless pump failures occur;

2. With the exception of operation with only two pumps in the same loop running, the design meets IEEE 279 criteria;

3. The probability that two pumps in the same loop will be out of service concurrently due to pump failure is low; and

4. The manual adjustments necessary to operate with two pumps in the same loop inoperable are made while the reactor is shut down.

Although we consider this design acceptable for the Oconee units, we are continuing to evaluate the B&W design, particularly in regard to the method in which the protection system set points are changed in preparation for single loop operation.

c. Reactor Coolant Flow Instruments

We have not completed our review of the reactor coolant flow instruments. A total of eight differential pressure transmitters are used to provide inputs to the reactor protection system. The four transmitters associated with each loop derive their input from the same flow nozzle and utilize the same two reactor coolant piping penetrations. We expressed our concern to the applicant that the design of the flow instruments did not meet the single failure requirement of IEEE 279. In its response, the applicant addressed only

the effects of a rupture of a single sensing line. We remain concerned that single failures (e.g., blockage of one penetration) could prevent all flow instruments in a loop from responding to a flow reduction. We expect to receive additional information on this matter from the applicant and will be prepared to report orally to the Committee.

We conclude that, except for the item discussed in c. above, the reactor protection system meets the proposed GDC and IEEE 279 and is acceptable.

Engineered Safety Feature Actuation System

The engineered safety feature actuation system consists of eight channels. Two independent actuation channels are provided for each engineered safety feature system.

The emergency core cooling systems, i.e., high pressure injection and low pressure injection, are actuated from the sensing of either low reactor coolant pressure or high containment pressure. The applicant has stated that, for some break sizes, a reactor trip is required for the emergency core cooling systems to be effective but diverse reactor trip signals have not been provided. The applicant's position is that the reliability of the low reactor coolant pressure signal makes a diverse reactor

trip signal unnecessary. We have informed the applicant of our conclusion that all functions required for effective emergency core cooling should be actuated from the sensing of diverse variables. We expect no additional information on this matter and will require that a diverse reactor trip signal be provided.

We have reviewed the schematic diagrams and the test procedures for the engineered safety feature actuation circuits with the applicant. In view of our concerns with the test capability provided by the Westinghouse design, we wish to point out some features of Babcock and Wilcox design. The entire system, from the sensors to the actuated components (e.g., pumps, valves) and including the bypass provisions, can be tested during reactor operation. During the periodic tests, the channel under test is not incapacitated and a valid trip signal will actuate both channels associated with each engineered safety feature system. Each actuated component has its own unit control module. The unit control modules are the equivalent of the Westinghouse slave relays except that each slave relay actuates several components. Although the B&W design, like the Westinghouse design, does not permit an integrated system test during reactor operation, the individual components can be actuated one at a time using the associated unit control module in a manner which adequately duplicates the action required under accident conditions. We conclude

that an acceptable means of completely testing the ESF actuation circuits during reactor operation is provided.

We conclude that, except for the lack of a diverse reactor trip signal, the engineered safety feature actuation system meets the proposed GDC and IEEE 279 and is acceptable.

Installation Criteria

We have reviewed the applicant's installation criteria relating to the preservation of the independence of redundant safety equipment by means of separation and to the prevention of fires through derating of power cables and proper tray loading. We have found these criteria to be acceptable. We intend to visit the site for the purpose of reviewing the implementation of these criteria after a majority of the protection system equipment has been installed.

Environmental Testing

In Section 6.1.2.12 of the FSAR, the applicant has listed the equipment which must be operable during and subsequent to an accident and has described some of the environmental tests performed on this equipment. We have reviewed this information and conclude that the test program is acceptable. However, we have requested the applicant to provide a brief description of the

tests used to qualify the sensors which provide input signals to the protection system. We expect to receive this information prior to the ACRS meeting and will assure ourselves that these tests adequately simulated the post-accident environment.

Seismic Design Criteria

The applicant's seismic design bases are that the protection systems shall function normally during and after either a maximum hypothetical earthquake or design earthquake. The protection system equipment is being dynamically tested to show normal operation during excitation in excess of the maximum predicted accelerations at its location through the frequency range expected during either earthquake.

We have evaluated the applicant's seismic design bases and conclude that they are acceptable.

EMERGENCY POWER SYSTEM

Offsite Power

Offsite power is available to each unit from the 230 kV switchyard via the three 230/4.16 kV startup transformers. Eight 230 kV transmission lines (four installed with Unit 1; two added with Unit 2; two added with Unit 3) converge at the site via

several rights-of-way. The 230 kV switchyard is arranged into a breaker-and-a-half configuration and each circuit breaker is provided with dual trip coils supplied from the two independent 125 Vdc station switching power systems. Circuit protection is provided by redundant relaying. Commencing with the operation of Unit 3, the 500 kV switchyard will be connected to the 230 kV switchyard via an autotransformer. The applicant has stated that the Duke system is designed to withstand the loss of any single generating unit within its network.

Our review indicates that the only portion of the offsite power system vulnerable to a single random failure is the single startup transformer for each unit. Prior to the operation of Units 2 and 3, the only source of offsite power for Unit 1 is via its startup transformer. We have accepted single startup transformers for three previous applications: Ginna, Robinson, and Palisades. This arrangement was accepted for those plants because of the reliability of such transformers. An additional consideration in the case of Oconee Unit 1 is the fact that the single startup transformer circuit will exist for only about one year. With the operation of Units 2 and 3, additional sources of power can be made available through manual breaker operations which connect another unit's startup transformer to the emergency buses of the affected unit.

Based on our review, we conclude that the offsite power system, while not fully meeting the proposed GDC 39, will meet draft Criterion 17 after Unit 2 begins operation and is acceptable.

Onsite Power

Onsite power for Units 1, 2, and 3 is provided by two hydroelectric plants rather than diesel generators as for other applications. Power from the hydro units is available via either the 230 kV switchyard and the Unit 1, 2, or 3 startup transformers or the 13.8 kV underground feeder which utilizes its own 13.2/4.16 kV transformer. Either hydro unit can supply sufficient power, via either circuit, for operation of the engineered safety feature loads of one unit plus the safe shutdown loads of the other two units.

Figure 8-2 of the FSAR shows the arrangement of the station's main buses. Three engineered safety feature 4.16 kV buses are provided for each unit and these buses are connected to both of the unit's 4.16 kV main feeder buses. The sources of power which are automatically connected to the main feeder buses, in the order that they are connected, are:

1. The 230 kV switchyard via the unit's startup transformer;
2. The preselected hydro unit via the 13.8 kV underground feeder and the station's standby buses; and
3. The other hydro unit via a 230 kV overhead line, the 230 kV switchyard and the unit's startup transformer.

The following sources of power can be made available manually:

1. Another Oconee unit via the standby buses;
2. Another Oconee unit's startup transformer via the station's emergency startup bus; and
3. One of the three gas turbines located 30 miles away at Lee Steam Station via an overhead 100 kV transmission line and the standby buses.

In evaluating these power sources, we have not considered the gas turbine as a power source except as a temporary substitute for the hydro units during the periods when the hydro units are not available. The applicant has estimated these periods to be approximately 24 hours each year plus four days every ten years when the common penstock will be drained for inspection and maintenance. During these periods, the gas turbine is manually connected to the standby buses via a 100 kV overhead transmission line which is separated from the transmission network.

While the Oconee system obviously has many sources of power available, an aspect of the design which would not be acceptable in a current construction permit application is the lack of independent load groups. Regardless of the source of power, the three redundant engineered safety feature buses are connected in parallel through the two main feeder buses. All other recently

approved facilities have provided two or more electrically independent load groups, each with its own source of emergency power (split-bus). We have asked the applicant to submit an analysis of the Oconee design to show that the independence and reliability of the redundant engineered safety features loads are comparable to the independence and reliability provided by a split-bus design. At present we believe that the applicant will be able to show that the Oconee design is acceptable based on the large number of power sources, the relatively large capacity of these sources, and the high reliability of the hydro units.

One feature of the onsite distribution system on which we and the applicant have been unable to reach agreement involves the automatic transfer of power to redundant motor control centers. As presently proposed, the three ESF 600 volt motor control centers receive power via an automatic transfer device from two of the three 4160 volt engineered safety feature buses. We asked the applicant to identify those loads which require this automatic feature in order to meet the design bases. The only load so identified is one of the three reactor building fan coolers. However, it appears that if one fan cooler were connected to each of the three ESF buses, the design bases would be met without automatic transfer. It is our opinion that the use of the automatic transfer feature unnecessarily reduces the

already limited independence of redundant engineered safety feature equipment. We will require that the design be changed to eliminate the automatic transfer of loads between redundant engineered safety feature buses.

The arrangement of the 125 Vdc Instrumentation and Control Power System for Unit 1 is shown in Figure 8-5 of the FSAR. Each of the four distribution panels associated with a particular unit receives power via diode assemblies from either of two 125 V battery buses, one in the associated unit and one in another unit. Therefore, the source of power to each panel is automatically transferred, albeit in a unique manner, between redundant buses. Our concerns with the use of automatic transfer devices connected between redundant d-c buses were most recently discussed in our report to the Committee on the Point Beach facility. Our conclusion that the Oconee design is acceptable does not conflict with our position that a split-bus design should be used. Our conclusion that the use of isolating transfer diodes is acceptable for the Oconee units is based on the following:

1. The failure (open or short circuit) of a single diode does not result in a loss of power to any bus or load;
2. Diode monitors, which are capable of immediately detecting an open or shorted diode, are provided for each diode assembly; and

3. If it is assumed that all overload devices fail to function, a single fault could result in the loss of power to one 120 Vac vital instrument bus, one 125 Vdc power panel and both battery buses which supply power to that d-c panel. The loss of power to these buses and their loads will not reduce the capability of the protection system below that required to meet the minimum safety requirements of any unit.

In summary, the Oconee design is unique in the respect that the large number of batteries, together with the capability of immediately detecting failures, provides a system which can withstand not only a loss of power to any single load group supplied via an automatic transfer device, but also the loss of both sources of power to the transfer device.

Based on our review, we conclude that, if the automatic transfer of power to the 600 V motor control centers is eliminated, the onsite power systems meet the proposed GDC 39 and are acceptable.