SAFETY ANALYSIS

Oconee, Units #1, 2, and 3

Instrumentation, Control, and Power

Instrumentation and Controls

a) Description

The reactor protection system automatically trips the reactor to protect the reactor core under the following conditions:

a) The reactor power, as measured by neutron flux, reaches an established maximum limit or the limit set by reactor coolant flow.

b) The startup rate reaches an established maximum limit.

c) Certain mismatch conditions exist between reactor coolant flow and the number of pump motor breakers in service.

d) The reactor outlet temperature reaches an established maximum limit.

e) The reactor pressure reaches an established minimum limit.

The reactor protection system automatically trips the reactor to protect the reactor coolant system under the following condition:

a) The reactor pressure reaches an established maximum limit.

The engineered safety features protection system automatically performs the following functions to mitigate the effects of a serious accident:

a) Initiates operation of the core emergency injection system upon detection of low reactor coolant pressure.

OFFICE ▶						
SURNAME ▶						
DATE ▶						

Form AEC-318 (Rev. 9-53)

U.S. GOVERNMENT PRINTING OFFICE : 1966—O-214-629

b) Initiates operation of the reactor building cooling systems upon detection of an abnormally high reactor building pressure.

c) Initiates containment isolation upon detection of an abnormally high reactor building pressure.

A schematic diagram of the reactor protection system is shown in figure 7-2 of the PSAR.

The nuclear instrumentation has eight channels of neutron information divided into three ranges of sensitivity: source range, intermediate range, and power range. The three ranges combine to give a continuous measurement of reactor power from source level to approximately 125% of full power, or ten decades of information. A minimum of one decade of overlapping information is provided.

The physical location of the neutron detectors is shown in figure 7-10 (PSAR). The power range detectors are located in four primary positions, 90 degrees apart around the reactor core. The three chambers associated with each power range channel are located near the top of the core, at the midplane, and near the bottom of the core. The two source range proportional counters are located on opposite sides of the core adjacent to two of the power range detectors. The two intermediate range compensated ion chambers are also located on opposite sides of the core, but are rotated 90 degrees from the source range detectors.

The source range channels utilize proportional counters and generate log count rate and startup rate (decades/minute) signals. There is no trip capability. However, the startup rate signals initiate control-rod-withdrawal-hold in response to high startup rate signals (1/2 logic).

The intermediate range instrumentation has two channels originating in two compensated ion chambers. Log N and startup rate information is derived. The startup rate signals initiate control-rod-withdrawal-hold and reactor trip, as appropriate (1/2 logic).

The power range instrumentation consists of four linear level channels originating in twelve uncompensated ion chambers. The gain of each channel is adjustable, providing a means for calibrating the output against a reactor heat balance. These channels combine power, flow, and pump breaker information and effect reactor trip (2/4 logic) under certain conditions.

There are two "flow tubes", one in each primary loop, as shown in figure 7-11 of the PSAR. Flow information is measured as a function of pressure drop by four independent sensors at each tube. The outputs of the eight sensors are combined as pairs such that four independent <u>total</u> flow signals are derived. Each total-flow signal is fed to one of the four power range channels, thus creating four independent power/flow channels. In addition,

each pump motor breaker has four contacts which are respectively connected to the four power/flow channels. Thus, each power/flow channel receives identical information.

The power/flow channels will initiate reactor trip if:

a) reactor power exceeds 107% F.P. under any conditions, or

b) the power/flow ratio exceeds 1.07 under any conditions, or

*c) one pump is lost as a result of a tripped pump motor breaker when operating above a predetermined neutron power level (X% F.P.), or

*d) one pump is lost for reasons other than tripping of its breaker (e.g., a sheared rotor) when operating above X% F.P., or

*e) two pumps are lost as a result of tripped pump motor breakers, and the ratio of reactor power to the steady state flow corresponding to the remaining pumps is greater than 1.07.

An automatic servo action, calling for a reduction in power to achieve a proper power/flow ratio, will occur when power is below X% F.P., and

a) one pump is lost due to tripping of its breaker, or

b) more than one pump is lost due to breaker tripping and the ratio of reactor power (at the instant of breaker trip) to the steady state flow corresponding to the remaining pumps is less than 1.07.

---

* Anticipatory trips

OFFICE ▶						
SURNAME ▶						
DATE ▶						

The above provisions allow the downward adjustment of reactor power to a level commensurate with the remaining pumps as a means of "keeping ahead" of the flow coastdown unless it is a foregone conclusion (as "judged" by the various comparator circuits) that the impending loss-of-flow transient is sufficiently severe to warrant immediate trip.

Reactor outlet temperature is monitored by eight resistance elements, four elements in each loop. Four of these, two in each loop, are connected to the reactor protection system (2/4 logic). The remaining four feed into the reactor control system.

Four force-balance transmitter devices measure reactor coolant system pressure. There are two transmitters at each loop. Their outputs are connected to the protection system and effect reactor trip upon coincidence of two high or two low pressure signals (2/4 logic).

As shown in figure 7-2B, all trip-producing channels (with the exception of Startup Rate) have four sensors whose outputs respectively interrupt current to four independent bistable units. Each bistable unit, in turn, interrupts one of four relays. The relay contacts are combined so as to de-energize the undervoltage coils of four circuit breakers which control the a.c. power input to the control rod drive system power supplies. A.C. input power is fed from two single phase sources, both of which must be interrupted to produce a reactor trip. The circuit breaker logic itself

is "one out of two-twice" (1/2 X 2), and responds to the instrument channels on a 2/4 logic basis (1/2 for the startup rate).

The d.c. outputs of the two rod drive power supplies, which are respectively controlled by the two s.c. lines described in the preceding paragraph, are connected in parallel through diodes to a common bus (Ref. fig. 3-59, PSAR). This bus supplies power to all sixty-nine rod clutches. Thus, reactor trip is accomplished by de-energizing the bus.

Manual trip is accomplished by directly de-energizing the undervoltage coils at the circuit breakers.

Two protection system channels also have a control function. The output of one of the four nuclear flux level channels is sent to the reactor servo system. Also, one of the four pressure sensors is used to control pressurizer pressure.

Instrument channels which initiate engineered safety feature action are distinct from those used in the protection system and have no control function.

Three pressure sensing channels (2/3 logic) start operation of the high pressure coolant injection system upon detection of low reactor coolant system pressure, and start operation of the low pressure injection system upon detection of very low reactor coolant system pressure.

Three other pressure sensor channels (2/3 logic) initiate reactor building emergency cooling and containment isolation upon receipt of high pressure signals.

Two additional sets of three pressure sensors (2/3 logic within each set) respectively initiate operation of one reactor building spray pump and associated valves.

As can be seen in figure 7-2c (PSAR), the final logic circuits feeding each safeguard are duplicated and redundant.

The incore instrumentation consists of 52 assemblies of self-powered neutron detectors, temperature detectors, and support tubes located at preselected positions within the core. This system provides neutron flux and temperature detectors to monitor core performance. There is no protection action or control function.

Each incore detector assembly consists of four local flux detectors, one background detector, two (inlet and outlet) temperature detectors, and a calibration tube. The flux detectors are positioned at four different axial elevations to provide the axial flux gradient. The background detectors, which are insensitive to neutron flux, provide a means of applying suitable corrections to the outputs of the active chambers should the signal to (background) noise ratio become too low.

Readout is performed by a data reduction system. This system sounds alarms if local flux conditions exceed predetermined values.

Reactivity control is maintained by movable control rods and soluble poison (boric acid) dissolved in the reactor coolant.

There are sixty-nine control rods, each of which is driven by a single phase synchronous stepping motor through an overrunning and an electromagnetic clutch. Twenty-five rods are used for automatic control purposes, the remaining forty-four being assigned as safety rods. Individual rod position readout devices are provided. There are two redundant position transmitters at each rod. "In" and "Out" limit information is also available.

For operational purposes, the control rods are divided into four groups. No more than one of these groups can be withdrawn at a given time except that, over the last twenty-five percent travel of one group and the first twenty-five percent travel of the next group, overlapping motion of the two groups is permitted.

The safety rods can be divided into as many as eight groups. These are withdrawn initially, one group at a time, and are controlled by manual means only.

All rods are driven at constant speed by means of a pulsing circuit which steps the synchronous motors with a.c. pulses of constant frequency and duration.

The automatic control (servo) system positions the control rods in response to magnetit demand, coolant system average temperature demand, and measured neutron flux signals. An error signal is generated which is the deviation between the total demand signal and the measured neutron flux. One of the four power range channels will provide the neutron flux signal.

The automatic control system will also, under certain conditions, reduce power upon loss of one or more pumps. This action has been discussed previously.

As fuel burnup progresses, dilution of the soluble poison is manually initiated and automatically terminated as follows:

When the partially withdrawn active control rod group reaches the fully withdrawn point, interlock circuitry permits setting up of a flow path from the dimineralized water tank, in lieu of the normal flow path of borated makeup, to the reactor coolant system. When the control group has been inserted to the seventy-five percent withdrawn position, the dilution flow is automtically blocked. The dilution cycle is also terminated when a flow integrator (not a timer, as stated in the PSAR) determines that a preset maximum amount of water has been injected.

b) Analysis

The applicant has stated that the instrumentation will be designed, built and tested in accordance with the proposed IEEE Standard for Nuclear Power Plant Protection Systems (Rev. 8). In addition, the applicant will design in accordance with the following specific criteria outlined in Section 7 of the PSAR:

a) No single component failure shall prevent the protection systems from fulfilling their protective functions when required.

b) No single component failure shall initiate unnecessary protective system action, provided implementation does not conflict with the above criterion.

c) All protection system functions shall be implemented by means of redundant sensors, instrument strings, logic devices and action devices which combine to form the protection channels.

d) Redundant protection system channels and their associated elements shall be electrically independent and packaged to provide physical separation.

e) A loss of a.c. power to the reactor protection system shall cause the affected channel(s) to trip.

f) Equipment is divided between the redundant engineered safeguards channels in such a way that the loss of one of the d.c. power busses does not inhibit the systems' intended safeguards functions. Loss of a.c. to the engineered safeguards system shall cause the affected channels to trip.

OFFICE ▶						
SURNAME ▶						
DATE ▶						

g) Manual trip shall be independent of the automatic trip instrumentation.

h) Preoperational and on-line testing capability shall be provided.

The basic design of the protection system is shown in figure 7-2 of the PSAR. The final reactor trip circuit is shown in figure 3-59.

All reactor trip instrumentation (with the exception of the "startup rate" channels) are coincident and redundant. Four independent channels monitor each "trip" parameter, and one (and only one) output of each channel controls four independent circuits which, respectively, control four independent relays (RS 1,2,3, and 4). The output of these relays are combined (2/4 logic) to operate four circuit breakers which de-energize the two a.c. input circuits feeding the rod drive (d.c.) power supplies. The circuit breaker logic is 1/2 X 2: i.e., a trip results if (at least) one of the two circuit breakers in one a.c. line and (at least) one in the other line are opened. Each a.c. line furnishes power to one of the clutches through diodes which permit testing of the final trip circuits during reactor operation.

Only one of the four nuclear power range channels will provide an input to the reactor control system. This is a departure from the original design which connected all four power range channels to the servo. The design now conforms to Section 4.7 of the IEEE Standard.

OFFICE ▶						
SURNAME ▶						
DATE ▶						

Our analysis of the power/flow instrumentation indicates that the design conforms to the current criteria. There are eight independent flowmeters, four in each primary loop as shown in figure 7-11. The flowmeter outputs are connected as four independent pairs (the flowmeters in each pair monitoring a different loop) such that they become four independent (total) flow channels. A flow channel is combined with only one of the power range channels. Independence is further preserved by feeding each of the four power/flow signals to only one of the four logic circuits.

These trip circuits which function as a result of abnormal pump breaker operation are designed to be immune to single electrical failures. Each breaker has four independent contacts which are respectively connected to one of the four power range channels. Thus, a failed contact will affect only one channel. However, a mechanical failure within a breaker (e.g., a breaker which failed to open even though power to its pump had been interrupted) would not be cancelled by system redundancy. Our analysis shows that this failure, or any similar failure involving pump breaker trip circuits, does not constitute a hazard inasmuch as the circuits provide only "anticipatory" trip functions and are always backed up by the "power/flow $>$ 1.07" circuits which would be effective under any conditions of pump motor loss.

The startup rate channels are effective only when reactor power is less than 10% of full power. Above 10% F.P. an operational bypass, actuated by the power range channels through 2/4 logic circuits, removes the startup rate trip function. Our analysis indicates that the two startup rate channels are independent, that no single failure, including a failure within the bypass removal circuits, can prevent their functioning.

There is one set of four pressure sensors and one set of four temperature sensors which trip the reactor on high and low primary system pressure, and high coolant outlet temperature. The logic is 2/4, and the instrument channels are independently connected to the four logic channels in the same manner as the power range channels. One pressure channel also provides a signal to the pressurizer pressure controller. The other three channels will provide trip action on a redundant basis should a common failure initiate a pressure transient and disable the one channel. This design conforms to the provisions of Section 4.7 of the proposed IEEE Standard (Rev. 8).

Operational bypass circuits within the low pressure portions of the protection system will conform to paragraph 4.12 of the IEEE Standard.

The four logic channels have been analyzed and found to be "fail safe" in the event of voltage loss, immune to single failures, and testable for credible faults.

OFFICE ▶						
SURNAME ▶						
DATE ▶						

The fail safety is inherent since the channels are tripped when de-energized. A partially or completely failed channel will disable only one "RS" relay. Action of the three remaining channels will open all four circuit breakers at the clutch power supplies. Action of only two of the remaining channels is actually required, and they will open at least one circuit breaker at each power supply. Testing for faults within a logic channel is straightforward; e.g., a short within a channel will be revealed when the bypassed contacts do not trip their RS relay when tested. Open circuits are self-revealing. Short circuits between channels can be detected by tripping the "high pressure" contacts one at a time (these are the contacts located furthest upstream). For example, a short between channels one and two will prevent RS1 from dropping out when "Hi Pressure #1" is tripped.

Our analysis of the final trip circuits (Ref. fig. 3-59) shows that they are fail safe, immune to single failure, and testable. The loss of one breaker in each a.c. line can be tolerated. Diode failure, open or shorted, will not prevent trip action. A "hot" short at the positive d.c. line will have no effect since the d.c. system is ungrounded. The system will be equipped with ground-fault detectors. Loss of a.c. and/or d.c. will cause, or tend to cause, reactor trip.

Testing at power is accomplished by tripping the circuit breakers one at a time and noting the absence of d.c. voltage at the appropriate power supply output just upstream of its isolating diode.

OFFICE ▶						
SURNAME ▶						
DATE ▶						

The manual trip switch contacts are in series with the four circuit breaker undervoltage coils. There is no dependence on instrumentation.

We agree with the applicant that his protection system design criteria are acceptable, and that the specific designs which are being proposed conform to these criteria.

Four sets of pressure sensing channels initiate the engineered safety features. Each set is coincident and redundant (2/3 logic). One set initiates the high and low pressure coolant injection systems. These six channels operate through amplifiers and bistable devices and are fail safe in terms of voltage loss. Two other sets of three channels respectively actuate the two reactor building spray systems. In these channels pressure switches are operated directly - there is no dependence on electrical power for switch operation.

Contacts controlled by the aforementioned channels are respectively combined into pairs of redundant logic chains which, in turn, control the safety feature systems. This is shown in figure 7-2a, PSAR. These chains are testable at power by means of two lights wired across the contacts of each chain such that the tripping of a chain produces a unique response from its lights.

Each redundant logic chain is energized from an independent d.c. power source.

Should a power source be lo , the downstream circuits fail "as is." However, we believe that system redundancy allows this condition to be defined as tolerable within the meaning of criterion #26.

The engineered safety features instrument channels do not control the parameters which they measure; i.e., there is separation of control and safety.

Manual actuation capability is provided.

We agree with the applicant's criteria and believe that the proposed design of the engineered safety features system properly implements these and all other applicable criteria.

The incore instrumentation system provides no automatic control or protection functions. The system is located entirely within containment, thereby precluding the need for isolation of penetrations associated with the system.

The control rod drives are being designed in accordance with detailed criteria stated on pages 3-65, 3-66, and 3-67 of the PSAR which can be summarized as follows:

a) "Single failures" shall be limited to one drive.

b) No single failure shall cause the uncontrolled withdrawal of any rod.

c) No more than two control groups can be withdrawn at one time.

d) The withdraw speed shall be limited so as not to exceed 25 percent overspeed in the event of speed control fault.

e) Continuous position indication shall be provided.

We agree with these criteria and have performed a failure mode analysis to determine the proposed system's degree of conformity to these criteria:

In order to determine the worst effect of "single failures" which might not be confined to a single rod drive, we asked the applicant to perform "startup accident" analyses covering the entire spectrum of initial power levels (Ref. Supplement 2, Question 4.9 and answer). This accident assumes the uncontrolled simultaneous withdrawal of all rods at maximum design speed, and further assumes that the excursion is terminated only by doppler feedback and trip action of the power range nuclear channels. The applicant concluded: "No fuel damage would result from simultaneous all-rod withdrawal from any initial power level."

From the preceding we have concluded that a single failure which allowed an extra rod group to be withdrawn, being of less severity than the accident analysed, would not cause fuel damage.

There will be two "speed limiting" features. One is the pulser (or clock) which will be designed not to exceed a certain maximum frequency. The

other is a "speed saturating circuit" downstream of the pulser which has the inherent property of not responding to a frequency greater than 125% of rated frequency.

There are two independent analog rod-position sensors at each rod drive, a potentiometer and an LVDT. There are two independent limit switches. In addition, the LVDT's will also generate limit signals. Thus, there are redundant analog and limit position indicating systems at each rod. Each analog signal at a rod can be fed into the individual rod position indicator.

We understand, at this writing, that a "drive-down, hold-down" mechanism in the form of an overrunning clutch will be installed at each rod drive. We agree with this decision.

Based on our analysis, we believe that the applicant's criteria conform to our own, that no single failure can produce an excursion which will breach the protection system, and that the proposed rod drive designs can be built in accordance with these criteria.

Reactivity is also controlled by a permissive system which allows manual dilution of the primary system coolant when a particular control rod group reaches the fully withdrawn point. Dilution is automatically terminated when the rod group, driven down by the servo, reaches a prescribed position, or when the integrated dilution flow has reached a preset maximum. We understand that these circuits will be designed in accordance with protection system standards.

OFFICE ▶						
SURNAME ▶						
DATE ▶						

We agree with the implied criterion that no single failure should prevent automatic termination of dilution, when required.

In summary, we conclude that the applicant's design criteria relating to instrumentation and controls are satisfactory and that the proposed preliminary designs conform to these criteria.

Power

Description:

Each unit will generate electric power at 19 kv which will be fed through an isolated phase bus to a unit step-up transformer (auxiliary transformer) where it will be raised to 230 kv for units 1 and 2, and 500 kv for unit 3. Two 230 kv overhead transmission lines will carry power between units 1 and 2 and the station switchyard which will be connected to the existing Duke 230 kv transmission line by six circuits: two north to Jocasse, two southeast to Central and (upon completion of Unit 2) two east-northeast to Tiger. From Unit 3, an overhead transmission line will carry power between the station and the switchyard which will be connected to Duke's 500 kv transmission network by two circuits: one to the Lake Norman area and the other to the Lake Wylie area, both being run in a general northeasterly direction. An autotransformer will tie together the 230 and 500 kv systems at the station switchyard. In addition, a separate 100 kv line will be run directly from the gas-turbine generating station at Lee.

Each unit will have its own 60 MVA startup transformer. The 100 kv line will terminate in a transformer at Oconee which will serve all three units, as required.

Normally, each unit will supply its own auxiliary loads directly from the generator via the station auxiliary transformer. Since each unit is being designed to accept a 100% load rejection, the primary source of

OFFICE ▶						
SURNAME ▶						
DATE ▶						

power for the auxiliary loads in the event of system blackout will be the unit generators themselves. In the event of a unit trip, the power sources will be automatically switched onto the auxiliary busses in the preferential sequence as follows:

a) the startup transformer bus

b) the other units' auxiliary electrical system (subsequent to the completion of Unit 2)

c) the 100 kv transmission line from Lee

d) the Keowee Hydro Station 13.8 kv line.

The Keowee Hydro Station will be located approximately one half mile from the station switchyard, and will consist of two 70 MWe generating units. Each unit is essentially independent of the other and is provided with its own startup equipment located within separate cubicles within the Keowee control room. The initiation of startup is accomplished by control signals from the Oconee control room areas. Normal startup of either unit is by operator action while emergency startup is automatic. Both units are started automatically and simultaneously on either of two conditions: if the external transmission system is lost or if engineered safeguards action is required.

Either hydro can be connected to either of two lines feeding the Oconee Station. One is an overhead 230 kv line to the station switchyard; the other is an underground 13.8 kv line run directly to a 10 MVA transformer.

Four 125 v.d.c. batteries and six battery chargers will be supplied for Unit 1. One pair of batteries and one set of three chargers will feed one 250/125 volt bus and the remaining pair of batteries and set of chargers will feed a redundant 250/125 volt bus (Ref. Fig. 8-3, PSAR). Upon completion of Unit 2, this d.c. system will serve both units. A third three-wire system will be installed upon completion of Unit 3. Switching circuits will permit any d.c. system to serve any unit.

Initially, there will be six 125 v.d.c. distribution panels, each of which will receive d.c. power from both three-wire d.c. sources through isolating diodes. Two more panels will be installed with Unit 3 and will be similarly powered. Four vital instrument busses (single phase) will be provided for Units 1 and 2, and will be independently energized from static inverters connected to one of the six d.c. distribution panels. Two more vital instrument busses will be added with Unit 3. These will be powered, through static inverters, from the two additional d.c. panels.

In addition, there will be three single phase 120 v.a.c. regulated instrument busses. These will normally be connected to the 600 v.a.c. busses of their own units through regulating equipment. Provision will be made to switch over to the vital instrument busses, if necessary.

Power - Analysis

Schematic diagrams of the electrical power systems are shown in Figures 8-1 and 8-3 of the PSAR.

Criterion #39 of the Commission's proposed General Design Criteria has served as the basis of our review of the off-site and on-site electrical power systems. In order to comply with the criterion, the off-site and on-site power systems must each, independently, withstand the failure of a single active component without loss of function.

Upon completion of Unit #1, off-site power will be available from the 100 kv system and from the 230 kv system which feed power into Oconee over separate transmission lines from Jocasse and Central. An additional 230 kv tie to Tiger will be installed upon completion of Unit #2; and, upon completion of Unit #3, a tie to Duke's 500 kv system will be installed. All off-site lines will be energized from several power generating stations, and the Duke system is designed to withstand the step-loss of any single generating unit within its network.

Redundant transformers will be available to distribute power to engineered safety feature loads. Transformer CT1 (to the 230 kv system) and transformer CT5 (to the 100 kv system) will be installed with Unit #1. An additional startup transformer will be installed with each of the other two units as they are completed, and each transformer will be able to energize the emergency loads of any unit.

In view of the foregoing and the fact that the Duke Power Company has never experienced a system-wide blackout, we agree with the applicant that the proposed off-site power sources and associated distribution equipment are sufficiently reliable for the intended purpose.

We cannot, however, determine that these collective off-site sources are immune to the adverse effects of single failures. Recent blackout experience elsewhere suggests that such immunity may not exist. Accordingly, and inasmuch as the the design and utilization of the on-site power sources are under the direct control of the applicant, we have analyzed the proposed on-site power system on the basis that the single failure criterion can and must be met.

Upon loss of the external grid, redundant voltage and frequency sensing devices on each of the 230 kv switching station busses will initiate, through separate and redundant channels, tripping of all 230 kv switching station isolation breakers, closing of all 230 kv switching station power supply breakers and startup of both Keowee units. They will synchronize and be connected to the 230 kv lines. One unit will also feed the 13.8 underground line. Shedding of non-essential loads (a requirement because of the limited capacity of the 13.8 kv/4.16 kv transformer) will be accomplished by circuit breakers with duplicate trip coils energized from different d.c. busses.

Upon loss of the external grid and the tripping of a given Oconee unit (caused, for example, by a DBA) the emergency power sources will be

SURNAME ▶						
DATE ▶						

U.S. GOVERNMENT PRINTING OFFICE : 1966—O-214-629

automatically switched onto the emergency (4.16 kv) busses of the affected unit in the following sequence:

a) the startup transformer bus

b) the other units' auxiliary electrical system, when available

c) the 100 kv line

d) the 13.8 kv underground line.

(Switching to (a) above will attempt to connect the emergency loads to the Keowee station via the 230 kv line.)

Our analysis indicate that the sequencing system described above is essential to plant safety since its failure could leave the emergency busses with no power. We have been assured that this system will meet the single failure criterion.

The Keowee hydro units can pick up emergency loads from black start in 23 seconds, which is adequate under DBA conditions. If tripped off line at full power due to a system disturbance, each unit can pick up full load in seven seconds. Each unit's voltage regulator is equipped with a volts-per-cycle limiting feature which permits it to accept load at the outset and thus drag the loads up to full speed in synchronism with its own acceleration. This serves to reduce the time required for the initiation of safeguards system action. We concur with the applicant that it is a desirable feature.

The hydro plant is started by opening gates which are powered by hydraulic accumulators. Stored hydraulic energy is sufficient for three full opening and closing cycles. Control circuits for emergency actuation of the accumulators will be redundant. A shear pin arrangement within the mechanical portion of the gate drive will release a jammed or otherwise fouled gate from the others.

The protection system on the hydro plant will be limited to only those parameters that will prevent geneation of power, such as generator insulation breakdown or loss of field.

In the event both hydro units must be shut down briefly for maintenance, emergency power can be made available to Oconee via the 100 kv line which can be isolated from the rest of the grid and kept continuously energized by one of the Lee station gas turbine generators set aside exclusively for this purpose. We believe this merits consideration even though it would allow a temporary non-redundant source of emergency power. We will continue to pursue this matter with the applicant and, at present, see no obstacle to eventual satisfactory resolution.

The engineered safety feature auxiliaries are provided with redundancy. To maintain this redundancy, the applicant has stated that these auxiliaries will be connected to redundant busses such that safety feature auxiliaries performing the same function are connected to different busses. Each of these busses is supplied from the redundant 4160 volt

main feeder busses which are, in term, supplied from the redundant sources described previously. We concur with the applicant in this design approach since it is an effective and simple way of implementing the single failure criterion (Ref. Fig. 8-1, PSAR).

Our review of the station battery system (shown in Fig. 8-3, PSAR) indicates that it is redundant and testable. Voltage at each of the panelboards, Dc-A, Dc-B. . .etc., is derived from redundant sources feeding through isolation diodes such that failure of one source does not affect the voltage at the panel board bus. Loss of voltage at a panelboard bus will not negate the d.c. system function.

Our review also indicates that no single failure can cause a loss of voltage at all vital instrument busses.

We have been informed by the applicant that means will be devised to test the diodes at power, and to determine (also at power) that no battery has become disconnected from its d.c. bus. We concure in these test procedures.

In summary, we agree with the applicant's proposed criteria for the design and implementation of the off-site and on-site power systems, and we further agree with the preliminary design approaches to implement these criteria.