AEC PDR
1 1 PDR
Shanauer
RSBoyd
RCDeYoung
DSkovholt
FSchroeder
RRMaccary
DKnuth
RTedesco
HDenton
PWR Branch Chiefs
RWKlecker
OGC
RO (3)
RMBernero - 2
Etoy - 2

Docket No. 50-313

FEB 7 1973

Mr. J. D. Phillips
Vice President & Chief Engineer
Arkansas Power & Light Company
Sixth and Pine Streets
Pine Bluff, Arkansas 71601

Dear Mr. Phillipe:

We recently performed our safety review of electrical, instrumentation, and control systems for the Arkansas Nuclear One - Unit 1 plant. On January 23, 1973, we met with your representatives and enumerated our conclusions and requirements. The enclosure to this letter documents and details our review findings and consequa. requirements which must be met for licensing.

Please inform us within seven (7) days after receipt of this letter of your intent to meet these conditions. If you cannot meet our specified date or if your reply is not fully responsive, it is highly likely that the overall schedule for completing the licensing review of this project will have to be extended. Your full response providing the manner by which you intend to meet these conditions should be submitted by March 15, 1973 in order for us to maintain our current review schedule which calls for issuance of our Safety Evaluation by April 23, 1973.

Please contact us if you have any questions regarding the enclosed positions.

Sincerely,

R. C. DeYoung, Assistant Director
for Pressurized Water Reactors
Directorate of Licensing

Enclosure:
Electrical, Instrumentation and Control
Safety Review Findings and Requirements

cc: Horace Jewell, Esquire
House, Holms & Jewell
1550 Tower Building
Little Rock, Arkansas 72201

DISTRIBUTION
Docket File - 1
PWR-4 Reading
RP Reading

OFFICE ▶			LR/ET+CB	PWR-4	L:C/PWR-4	L:AD/PWR
SURNAME ▶			JAC FOR VM VMoore	RMB RMBernero:kf	AS ASchwencer	RCdeYoung
DATE ▶			2/7/73	2/7/73	2/7/73	2/7/73

Form AEC-318 (Rev. 9-53) AECM 0240

☆ U. S. GOVERNMENT PRINTING OFFICE: 1972-466-983

8004220 909 E

UNITED STATES
ATOMIC ENERGY COMMISSION
WASHINGTON, D.C. 20545

Docket No. 50-313

FEB 7 1973

Mr. J. D. Phillips
Vice President & Chief Engineer
Arkansas Power & Light Company
Sixth and Pine Streets
Pine Bluff, Arkansas 71601

Dear Mr. Phillips:

We recently performed our safety review of electrical, instrumentation, and control systems for the Arkansas Nuclear One - Unit 1 plant. On January 23, 1973, we met with your representatives and enumerated our conclusions and requirements. The enclosure to this letter documents and details our review findings and consequent requirements which must be met for licensing.

Please inform us within seven (7) days after receipt of this letter of your intent to meet these conditions. If you cannot meet our specified date or if your reply is not fully responsive, it is highly likely that the overall schedule for completing the licensing review of this project will have to be extended. Your full response providing the manner by which you intend to meet these conditions should be submitted by March 15, 1973 in order for us to maintain our current review schedule which calls for issuance of our Safety Evaluation by April 23, 1973.

Please contact us if you have any questions regarding the enclosed positions.

Sincerely,

R. C. DeYoung, Assistant Director
for Pressurized Water Reactors
Directorate of Licensing

Enclosure:
Electrical, Instrumentation and Control
Safety Review Findings and Requirements

cc: Horace Jewell, Esquire
House, Holms & Jewell
1550 Tower Building
Little Rock, Arkansas 72201

ELECTRICAL, INSTRUMENTATION AND CONTROL

SAFETY REVIEW FINDINGS AND REQUIREMENTS

ARKANSAS NUCLEAR ONE - UNIT 1

DOCKET NO. 50-313

1. Reacto[illegible]n System (RPS)

The installed reactor building pressure protection sensors provide an analog output signal rather than a digital signal as documented in the FSAR and the "as built" RPS logic schematics. We do not know how you will modify the design to correct this inconsistency. However, since either design can be designed to meet the requirements of IEEE-279, we believe the inconsistency can be readily resolved and should not be a cause for further concern.

2. Engineered Safety Features (ESF) Actuation System

We have reviewed all aspects of the ESF actuation system, including logic schematics, testing capabilities and control of bypasses, and concluded that this system is acceptable, conditioned on the satisfactory implementation of the following design omission:

The present design of the ESF actuation system does not provide for initiating the isolation of the reactor building ventilation system nor the operation of the reactor building

penetration room ventilation system. In addition, lack of information has prevented us from reviewing the adequacy of the instrumentation and controls for these two ESF ventilation systems. We will require that the design of the ESF actuation system be modified to include these missing initiating features and that these features as well as the ventilation systems control circuits meet the criteria for similar ESF systems which include compliance with IEEE-279.

3. ESF Actuator Circuits and Related Equipment

We have reviewed the actuator control circuits and related equipment pertaining to the ESF systems, and concluded that the designs conform to our criteria and are acceptable, except for the following items:

3.1 Air-Operated Valves

Although ESF air-operated valves do not require air pressure to open or close upon an ESF trip signal, it appears from reviewing the electrical schematics and functional piping and instrument diagrams (P&IDs) that there are some valves which require air to operate. We have requested that you verify this and if it is determined to be correct, we will require that the design be made to conform to the criteria.

3.2 Valve Torque Switch Interlocks

The open and close control circuits of all ESF motor-operated valves are provided with torque switch interlocks. These interlocks will stop valve movement when the torque exerted by the valve-motor unit exceeds the setting of the torque switch. This event normally occurs upon the valve reaching the fully open or close position. These valves are normally either fully open or closed and a high initial torque is required to start valve movement. Thus, to prevent a torque switch from blocking valve movement, it is momentarily bypassed during the first 5% of travel with a valve position limit switch. However, there are no provisions to bypass the torque switches when the valve is at an intermediate position, and it

is not evident if the high starting torque will trip the torque switch precluding further movement of the valve from this position. Although the design of the control circuits prevents these valves from stopping at an intermediate position, it is our concern that a momentary loss of power may cause these valves to stop at an intermediate position and it is not evident that upon restoration of power these valves will ever reach the final destination. Your staff has agreed to examine this aspect of the design. If it is determined that the operation of the torque switch precludes starting valve movement from an intermediate position, we will require that the design be modified to correct this situation.

3.3 Decay Heat Removal System (DHRS) Overpressure Protection Interlocks

The motor-operated suction valves interlocks used to prevent over-pressurization of the DHRS by the Reactor Coolant System do not conform to the criteria stated in the licensing position for high pressure to low pressure interfaces. The following criteria were identified to your staff during our review:

a. At least two valves in series shall be provided to isolate the low pressure system.

b. For systems where both valves are motor-operated, the valves shall have independent and diverse interlocks to prevent valve opening at high pressure. These interlocks shall be designed to comply with all the requirements of IEEE-279.

c. Automatic closure of the motor-operated valves whenever the primary system pressure exceeds the pressure rating of the low pressure system. The closure devices shall be designed to comply with all the requirements of IEEE-279.

Your staff has agreed to modify the design to conform with the stated criteria. We will require that the design be submitted for our review prior to fabrication and installation in the plant.

3.4 Core Flooding Tank Isolation Valves

You have elected to open the breakers supplying power to the core flooding tank motor-operated isolation valves in order to ensure against accidental closure of these valves during normal reactor operation. Based on this mode of operation, your staff has been advised that the proposed administrative controls do not provide sufficient assurance that these valves will be open when required. We will require that the valve control circuits be designed to meet IEEE-279 and the following features be incorporated in the design:

a. Valve position visual indication (open or closed) in the control room for each valve which is not dependent on power being available to the valve actuator.

b. Valve-not-open audible alarm in the control room for each valve, actuated when the valve is not in the fully open position and reactor coolant pressure is above a preset value.

c. Valve position indications both visual and audible to be derived from redundant and independent valve position sensors and circuitry, such as limit switches actuated by the valve motor operator and valve position limit switches activated by stem travel. The reactor coolant pressure signals shall also be redundant and independent.

d. A Technical Specification requirement that the reactor shall not be made critical or shall be shutdown unless each core flooding tank isolation valve is open and the breaker supplying power to valve operator is locked open and tagged.

4. Auxiliary Systems Supporting ESF Systems

4.1 Pump-Motor Bearing Cooling Failures

It is not evident that the auxiliary systems providing lubricating oil and cooling water to ESF systems motor and pump bearings are essential to the proper functioning of the ESF systems. Your staff has been requested to determine if the loss of bearing

cooling will impair the operation of the ESF systems for the length of time required. If the consequences of failure are unacceptable, we will require that the instruments and controls for these supporting systems be designed as reliable as those for ESF systems that they support including compliance with the objectives of IEEE-279.

4.2 Switchgear Rooms Cooler Failure

The two pairs of redundant and independent ESF switchgear room coolers are being powered from the same bus. A failure of this bus will cause the loss of cooling capability in both of the switchgear rooms. We will require that you either demonstrate that the loss of cooling will not impair the proper functioning of the switchgear, or modify the design to supply power to each pair of room coolers from independent buses.

5. Separation and Identification Criteria for Protection and Emergency Power Systems

We have reviewed your criteria for separation and identification of cables and examined the design arrangement of these as well as other safety-related systems. We have found that these criteria and design arrangements are acceptable, except for the items listed below and under Item 7 which follows.

5.1 Reactor Coolant Pressure Sensors

Two of the three redundant coolant pressure sensors associated with the ESF actuation system are mounted on a common instrument rack. We will require that these sensors be separated unless you can demonstrate acceptability on the bases that diverse instrumentation provides equal protection.

5.2 Watertight Doors

The doors separating adjacent redundant ESF equipment rooms are not of the watertight construction such as in the diesel-generator and 4160 V switchgear rooms. It is our concern that the break of a service water supply line in either room may cause the flooding of both redundant rooms. We require that you examine each ESF equipment room and either demonstrate that this is not possible or modify the present design to prevent this occurrence from happening.

5.3 Battery Room Ventilation

The exhaust duct emanating from one of the 125 volt d-c station battery rooms passes through the other redundant battery room. It is our concern that a fire and/or explosion in this room could be propagated to the other room resulting in the loss of both redundant 125 volt d-c systems. Unless you can demonstrate the capability of this exhaust duct design to withstand these types of events, we require that the design be modified to assure complete independence of these ventilation systems.

6. Emergency Feedwater (EF) System

You have not identified the safety significance of the EF system to remove reactor decay heat in the event of a steam system failure concurrent with the loss of offsite power. Moreover, only manual means are provided to close the steam block valves upon a failure of the Category II piping of both main steam lines during an assumed major seismic event. You have not demonstrated that manual actuation is adequate to assure timely closure of the steam block valves. Therefore, we cannot evaluate the suitability of the present design until the safety significance of this system and related items is established. However, it should be noted that the present design of the EF system does not meet the single failure criterion in such areas as physical installation of equipment, power sources, and actuator circuits. Further, the Integrated Control System (ICS) participates in the operation of the EF system and it should be also noted that the ICS is not designed to meet IEEE-279. We consider the whole subject of I&C of the EF system including the steam system failure as an area of concern that must be resolved.

7. Control Room and Rod Drive Control (RDC) Equipment Room

Our review of the control room and RDC equipment room design arrangements revealed the following items of concern:

7.1 Control Room Subfloor

The RPS equipment cabinets are located in the control room and mounted on a raised floor. Cables entering the RPS cabinets are routed under the raised floor. It appears that the design arrangement of redundant RPS cables underneath the raised floor disregards any need for physical independence as provided in other areas through which these cables are routed. This cable design arrangement is considered to be vulnerable to common

mode failures resulting from design basis events such as fire and flooding. Furthermore, this apparent lack of cable separation and vulnerability to common mode failures is inconsistent with your own criteria as documented in the FSAR which include compliance with IEEE-279 and IEEE-308. Although we recognize the inherent fail-safe characteristics of the RPS upon loss of power, we cannot conclude that all failures will make the system fail in a safe manner. We will require that you either demonstrate the adequacy of this design against all design basis events or modify it to provide the required physical independence of the redundant protection systems.

7.2 Computer Room Subfloor

The Rod Drive Control (RDC) equipment cabinets, located in the computer room above the control room, are also mounted on a raised floor. The cable design arrangement underneath the raised floor is of concern for the same reasons stated before for the RPS cables. Although we recognize the inherent fail-safe characteristics of the system causing the rods to drop by gravity into the core upon loss of power, we cannot conclude that all failures will result in a safe shutdown of the reactor. We will require that you either demonstrate the adequacy of this design against all design basis events or modify it to provide the required physical independence between safety-related cables.

7.3 Control Room Overhead

Open raceways containing RDC power cables each carrying 47 A are located overhead in the control room. These power cables are a potential source of fire that could result in not only the loss of Unit 1 control room, but also the future adjoining Unit 2 control room. Your staff has claimed that the cables are derated and only half of these cables will be carrying 47 A at any one time. We have concluded that this cable design does not minimize the probability and effect of fires in the control room as required by AEC General Design Criterion (GDC) No. 3. We will require that you install a fire barrier separating these open raceways from the control room proper, and provide adequate accessibility and means necessary to extinguish a fire.

7.4 Control Room Coolers

The control room emergency air-conditioning unit is situated near and in direct line with cabinets containing RPS and ESF controls. It is our concern that the failure of the air-conditioning unit could cause mechanical or flooding damage to nearby redundant safety-related components. This could result in the loss of protective function capabilities. You should analyze these events and if it is determined that the consequences of this type of failure are unacceptable, we will require that you either provide positive means to prevent these events from happening or relocate the unit.

8. Use of Diesel Generators for Peaking

You have stated your intention to use the standby power supply diesel generator sets to supply power to the electrical system during peak load demand periods. We have questioned and discussed this subject with you indicating that frequent and prolonged paralleling of the preferred (offsite) and standby power supplies is contrary to providing the independence required by GDC 17 and IEEE-308. GDC 17 requires that provisions be included to minimize the probability of losing electrical power from any of the remaining supplies as a result of, or coincident with, the loss of the main unit generator, the loss of power from the grid (offsite preferred power supplies), or loss of power from the onsite (standby) power supplies. In addition, although IEEE-308 does not prohibit the use of diesel generators for other purposes, this Standard requires that the preferred and standby power supplies shall not have a common failure mode. Common failure is defined as: "A mechanism by which a single design basis event can cause redundant equipment to be inoperable."

Our review of the intended use of diesel generators for system peaking leads us to conclude that the required frequent interconnections of the preferred and standby power supplies do not minimize the probability of their coincident loss nor can the design be made immune to failure from a common failure mode. We also conclude that the economic gain does not justify the increased risk to safety resulting from operating the emergency

power systems in this degraded manner. Therefore, based on our interpretation of GDC 17 and IEEE-308, Section 5, Item 5.2.1(5), we will require that the diesel generator sets not be used for purposes other than emergency power supplies for the plant.

9. Offsite Power Connections

Our review of the electrical schematics revealed indiscriminate tripping of available offsite power supplies and apparent single failures resulting in the loss of both offsite and onsite power to the ESF buses. These problems are a direct result of the complexity of the control circuit design provided to accommodate system peaking operation with diesel generators. In view of the above, and the position confining the use of diesel generators, we require that you perform an overall audit of the present emergency power system design, and modify it as necessary to provide the independence of the power supplies required by GDC 17 and IEEE-308.