JAN 2 2 1973

Docket No. 50-286

Consolidated Edison Company
of New York, Inc.
ATTN: Mr. William J. Cahill, Jr.
Vice President
4 Irving Place
New York, New York 10003

Gentlemen:

As part of our continuing review of your application for an operating license for the Indian Point Nuclear Generating Unit No. 3, we met with your representatives on November 10, 1972 to review in detail the instrumentation, control, and electrical schematic drawings of these systems. During the course of this meeting we discussed with your representatives a number of areas in which the design of those instrumentation, control, and electrical systems related to safety did not appear to meet our design criteria or requirements.

Upon further review we have made a determination of those systems that may require modifications. The enclosure lists the affected systems, delineates our positions, and gives the basis for each position.

It will be necessary that you amend your FSAR to state clearly your position regarding compliance with each of these requirements. We are prepared to meet with you to discuss any of our positions if you believe further discussion is necessary. If such a meeting is needed, we request that your position on each of these matters and your specific questions regarding our requirements should be provided to us prior to such a meeting.

Our tentative review schedule is based on the assumption that this additional information will be available for our review by February 26, 1973. If you cannot meet this date, please inform us within seven (7) days after receipt of this letter so that we may revise our scheduling.

Sincerely,

Original signed by R. C. DeYoung

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

Enclosure:
AEC Requirements -
Instrumentation, Control,
and Electrical Systems

cc: LeBoeuf, Lamb, Leiby, & MacRae
ATTN: Arvin E. Upton, Esq.
1821 Jefferson Street, N.W.
Washington, D. C. 20036

DISTRIBUTION:
AEC PDR
Local PDR
Docket
RP Reading
PWR-1 Reading
PWR-1 File
SHanauer
RSBoyd
RCDeYoung
DSkovholt
FSchroeder
RRMaccary
DKnuth
RTedesco
HDenton
PWR Branch Chiefs
RWKlecker
OGC
RO (4)
HSpecter
JLee
VMoore
RPollard

OFFICE ▶	PWR-1	PWR-1	AD/PWRs			
X7401 SURNAME ▶	HSpecter:rw	DBVassallo	RCDeYoung			
DATE ▶	1/22/73	1/22/73	1/22/73			

AEC REQUIREMENTS

INSTRUMENTATION, CONTROL, AND ELECTRICAL SYSTEMS

INDIAN POINT NUCLEAR GENERATING UNIT NO. 3

1. Automatic Transfer Circuits

Your response to Question 8.2 describes the automatic transfer circuits that are provided for the diesel generator control circuits and the 480 volt switchgear breaker control circuits. You state that the automatic transfer circuits have been provided "in order to provide a reliable 480 volt safeguards system" and that the transfer scheme meets the intent of Safety Guide 6. We have concluded that the need for automatic transfer results from the incompatibility between the number of a-c power sources (three diesel generators) and the number of d-c power sources (two 125 volt batteries). We have also concluded that the design does not conform to Safety Guide 6 and that the automatic transfer circuits compromise the independence between redundant safety systems. The following position is similar to that taken on other recent operating licensing cases.

It is required that the d-c power system used to control the diesel generators and the 480 volt switchgear be designed without use of automatic circuit transfers between redundant power sources.

2. Switching From Injection Phase to Recirculation Phase

Pages 6.2-11 through 6.2-15 of the FSAR contain a description of the procedure used to change from the injection phase to the recirculation phase following a loss-of-coolant accident. Our review has disclosed that, in the event of an accident, the consequences of a single mispositioned switch are unacceptable. For example, if either "Switch Six" or "Switch Eight" is closed, all three high pressure safety injection pumps are disabled, either because their circuit breakers will not remain closed or because their common suction line is isolated. We consider this arrangement to be in violation of the single failure criterion. In addition, the design appears to violate the applicant's criteria in that operation of these switches negates a design feature intended to prevent the operator terminating a safety injection signal until after the auto-start sequence is completed.

It is required that automatic initiation of the operation of engineered safety feature systems be designed in accordance with the single failure criterion. The present design of the circuitry used to change from the injection phase to the recirculation phase is unacceptable because it does not conform to this requirement, i. e., any one of several switches, if not properly positioned, could prevent automatic initiation of redundant safety equipment.

3. Safety Injection Bypass

The safety injection system is designed to permit bypassing the low pressurizer pressure/low pressurizer level initiation signal. A single switch is provided to accomplish this bypass in both redundant initiation circuits. We consider this to be a violation of single failure criterion.

It is required that the circuitry used to bypass the low pressurizer pressure/low pressurizer level safety injection signal be designed in accordance with IEEE Std 279-1968. The present design does not conform with this requirement because of the use of a single switch common to both redundant initiation circuits.

4. Lack of Independence Between Redundant Safety Injection Pumps

The description of the high pressure injection system presented in the FSAR implies that the system is capable of performing its function even in the event of failure of any one of the three pumps. The FSAR does not describe the following design feature which was disclosed during the schematic drawing review: If either pump 31 or pump 33 fails to start, the discharge valves for pump 32 are repositioned. The applicant stated that it is not known whether or not the system performance is adequate if the valves are not repositioned correctly. We consider this to be a violation of the single failure criterion.

It is required that engineered safety feature systems be designed in accordance with the single failure criterion. The adequacy of the single failure criterion is based in part on the assumption that neither operation nor failure of one component will interfere with proper operation of its redundant counterpart. Therefore, it is required that either:

a. An analysis be performed to demonstrate that any combination of two high level safety pumps is adequate assuming that valves 851A and 851B shown in FSAR Figure 6.2-1 are open and that the third high head safety pump is inoperable; or

b. Those portions of the protection system and safety injection system that are used to detect failure of one pump and subsequently change operation of the remaining two pumps be designed in accordance with the single failure criterion.

5. Bypass of Redundant Engineered Safety Feature Systems (ESF)

The testing scheme for the ESF actuation circuits requires bypassing the automatic initiation function. As described in the response to Question 7.10, there are no positive means, such as an interlock, to prevent bypassing both redundant circuits. In addition, the bypass indication does not identify which of the two circuits is bypassed nor can the operator distinguish between bypass of one and bypass of both circuits. We have concluded that this arrangement is not in accordance with Safety Guide 22 and violates Section 4.13 of IEEE Std 279-1968.

It is required that the protection system be designed such that, either:

a. Positive means are provided to prevent concurrent bypasses of redundant safety equipment and each bypass is uniquely indicated on the main control board; or

b. Indication is provided on the main control board to uniquely identify the portion of the system that is bypassed and to alert the operator to the need for immediate corrective action if redundant portions are bypassed concurrently.

6. Disconnection of Fuel Oil Transfer Pumps

All three diesel fuel oil transfer pumps are connected to non-safety buses and are disconnected from their electric power supplies in the event of an accident or loss of offsite power. We consider this a violation of Section 5.2.2 (5) of IEEE Std 308-1971 which requires that auxiliary devices be supplied from a Class IE bus that is related to the Class IE buses of the dependent equipment.

It is required that all equipment necessary for operation of the diesel generators be supplied from Class IE buses related to the load groups served by the diesel generators.

7. Fuel Oil Transfer System Control Circuits

The design of the control system for the fuel oil transfer system is described in the applicant's response to Question 8.4. We have reviewed the design and concluded that the automatic control system does not meet the single failure criterion. We also find unacceptable the proposed procedure which requires the use of "jumpers" to bypass failed components in the automatic circuit. We agree with the applicant that automatic control is not required because of the time available for manual control of the fuel oil transfer system.

It is required that the fuel oil transfer system be designed such that either the automatic or the manual control mode meets the requirements of IEEE Std 279-1968. If you choose the latter, it is required that permanently installed equipment be provided to change operation of the system from automatic to manual control. The use of "jumpers" as described on FSAR page Q8.4-2 is unacceptable.