

DUKE POWER COMPANY

P.O. BOX 33189
CHARLOTTE, N.C. 28242

HAL B. TUCKER
VICE PRESIDENT
NUCLEAR PRODUCTION

TELEPHONE
(704) 373-4531

January 14, 1983

Mr. Harold R. Denton, Director
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Attention: Ms. E. G. Adensam, Chief
Licensing Branch No. 4

Re: Catawba Nuclear Station
Docket Nos. 50-413 and 50-414

Dear Mr. Denton:

Elinor G. Adensam's letter of December 30, 1982 requested a response to four concerns from the Instrumentation and Control Systems Branch. Each of these concerns had been discussed in detail with the NRC Staff at review meetings held during the course of the ICSB review of Catawba. Attached are responses to each of the ICSB concerns.

Very truly yours,

Hal B. Tucker

Hal B. Tucker

ROS/php
Attachment

cc: Mr. James P. O'Reilly, Regional Administrator
U. S. Nuclear Regulatory Commission
Region II
101 Marietta Street, Suite 3100
Atlanta, Georgia 30303

Mr. P. K. Van Doorn
NRC Resident Inspector
Catawba Nuclear Station

Mr. Robert Guild, Esq.
Attorney-at-Law
P. O. Box 12097
Charleston, South Carolina 29412

Palmetto Alliance
2135½ Devine Street
Columbia, South Carolina 29205

3001

Mr. Harold R. Denton, Director
January 14, 1983
Page 2

cc: Mr. Jesse L. Riley
Carolina Environmental Study Group
854 Henley Place
Charlotte, North Carolina 28207

Mr. Henry A. Presler, Chairman
Charlotte-Mecklenburg Environmental Coalition
943 Henley Place
Charlotte, North Carolina 28207

INSTRUMENTATION AND CONTROL CONCERNS
FOR CATAWBA

1. In our latest discussions with the applicant, it was indicated that the miniflow valves (ND 25A and 59B) for the RHR pumps have uniquely configured control switches. Both switches have a momentary "OPEN" position which, when pressed, open the corresponding valve. The switches, when in their maintained "AUTO" positions, permit the individual valves to close on either a high pump discharge flow or a RHR pump not running signal from their associated pumps. Additionally, in the "AUTO" position, the individual valves open on a low pump discharge flow and pump running signal from their associated pumps. The unique feature of these switches is the release bar which, when pressed, takes the switch out of "AUTO" but does not place the switch in "OPEN." In this neutral position, the miniflow valves cannot change positions until their switch is placed either in the "AUTO" OR "OPEN" position.

CONCERN:

The staff is concerned that if the control switches are left in the neutral position, the miniflow valves will not respond to an automatic open signal required for RHR pump protection. This would appear to be a means by which both pumps could be damaged on a SI, if the minimum flow protection is not in the automatic mode. Provide a discussion on how this issue will be resolved for Catawba.

RESPONSE: Modifications will be made to the control circuits for valves ND25A and ND59B such that the valves will open upon a Residual Heat Removal pump running signal coincident with low pump discharge flow regardless of switch position selected. This will assure the availability of the valves to open to provide miniflow protection for the pumps.

2. In recent discussions with the applicant, it was indicated that if the safety injection reset timer or the diesel sequencer fail, manual reset of the sequencer may be prevented or the sequence may not be completed. Under these conditions the operator is prevented from possibly manually initiating ESF loads or manually tripping ESF loads unless he removes power from the sequencer in order to regain manual control or takes action to control individual loads at the switchgear.

CONCERN:

The staff is concerned that under accident conditions, as well as inadvertent initiation of load sequence programs, the inability of the operator to exercise manual control could lead to consequential damage of safety related equipment or prevent initiation of protection systems. As an example, the RHR pumps are protected by miniflow bypass valves which open following a pump start. If one of these valves fails to open, the operator cannot turn the associated pump off in the event of a sequencer failure without opening breakers or removing fuses. Similarly, the same situation can occur for the NSW pumps which are protected from loss of suction by transfer of intake from Lake Wylie to the SNSWP. While it is recognized that conditions which could lead to equipment damage would require more than a single failure, the types of multiple failures required are not limited to those associated with independent, redundant trains of protection equipment. Thus, it is concluded that the fault tolerance of the system design and specifically the potential for the operator

to be incapable of exercising manual control introduces a safety significant issue.

Therefore, provide your rationale that the design is acceptable in light of these concerns and/or any specific actions which will be taken to address these concerns.

RESPONSE: The Catawba Diesel Generator Load Sequencer receives actuation signals from the Solid State Protection System (SSPS) and actuates Engineered Safety Feature (ESF) components in a manner which is consistent with both the safety analysis and the diesel generator loading capability. As such the sequencer can be thought of as an extension of the protection system and was designed considering the features of and criteria for the protection system.

According to paragraph 4.16 of IEEE 279, "The protection system shall be so designed that, once initiated, a protective action at the system level shall go to completion. Return to operation shall require subsequent deliberate operator action."

Consistent with this guidance the Safety Injection Actuation portion of the SSPS which actuates the sequencer is designed with a reset switch requiring deliberate operator action to return to normal operation. A minimum reset timer has been included in the design which insures that the protective action carries through to completion.

The sequencer design employs similar features. Consistent with the minimum reset timer feature of the SSPS the sequencer cannot be reset until the SSPS is reset. Manual operation is inhibited during this interval insuring that protective actions go through to completion in accordance with IEEE 279 guidance. If manual operation were not inhibited during this interval the SSPS minimum reset timer feature could be essentially defeated. This also precludes the possibility of automatic sequencing and manual loading occurring simultaneously causing incorrect sequencing or diesel generator overloading or failure.

Once the SSPS is reset, sequencer return to normal operation requires deliberate operator action through use of the sequencer reset switch.

Paragraph 4.2 of IEEE 279 defines the single failure requirements for a protection system. The design of the sequencer incorporated this guidance. The multiple failures postulated by the staff are beyond the requirements stated for any protection system. It should be noted, however, that even with the failures postulated in this concern the protective function is still accomplished by the redundant train.

The design of the Catawba Diesel Generator Load Sequencer extends the philosophy of the SSPS to the entire ESF actuation system and is consistent with the guidance provided in IEEE 279.

3. One of our previous concerns pertained to the loss of both trains of RHR due to a single instrument bus failure. In our past discussions, the applicant has stated that the operator is informed that he has lost RHR by low flow alarms, that there is enough time to manually re-establish RHR, and that the operator knows what action to take under these circumstances. Additionally, miniflow valves are provided to prevent pump damage.

CONCERN:

The staff is still concerned that the loss of both trains of RHR during decay heat removal is a safety significant issue. Therefore, a written response should be provided to document the applicant's position that this is not a safety problem, to discuss the importance of time in re-establishing RHR, and to discuss what (training, procedures, etc.) specifically tells the operator how to respond to this situation.

RESPONSE: In the Residual Heat Removal mode of operation the RHR pumps are connected to the reactor coolant system through one or both of two parallel suction lines. Since the RHR piping has a significantly lower design pressure than the reactor coolant piping, each suction line is provided with redundant (one Train A, one Train B) isolation valves which isolate automatically upon reaching a predetermined reactor coolant pressure setpoint.

Since both lines contain a Train A isolation valve and a Train B isolation valve actuation of either Train will cause isolation of the RHR piping from the reactor coolant piping. Additionally the failure mode of the isolation logic is such that the safety mode (i.e. isolation) is achieved upon loss of an instrument bus to either the Train A or Train B logic.

Upon loss of an instrument bus while in the Residual Heat Removal mode of operation, the suction lines will isolate and RHR operation is terminated. Once the suction lines are isolated RHR discharge flow will decrease and the pump miniflow valves will automatically open.

Adequate alarms are provided to the operator to identify the loss of RHR. The operator will then trip the RHR pumps and take action to reinitiate decay heat removal by reestablishment of the RHR system lineup or by establishing cooling through the steam generators. Adequate time is available for the operator to take the necessary actions to reestablish decay heat removal.

As addressed in Section 13.5.2.1.2 of the Catawba FSAR, emergency procedures will be generated to address the operator response to a loss of residual heat removal.

Due to the safety significance of a loss of isolation between the RHR piping and the reactor coolant piping while the reactor coolant system is at normal operating pressure, the failsafe mode (i.e. isolation) upon power loss of this actuation logic is appropriate. This adds reliability to the isolation function and makes it more secure to events such as fires, etc.

4. Logic diagrams for the auxiliary feedwater pump suction alignment to the NSW system are shown in FASR Figures 7.4.1.1 and 7.4.1.2. The logic is complex, containing multiple coincidence logic and several time delays.

CONCERN:

The staff is concerned about the testability of the alignment logic during power operation. Provide a discussion describing how this circuitry will be tested at power.

RESPONSE: Instrumentation and logic associated with the nuclear service water (RN) swapper to the auxiliary feedwater (CA) system will be tested and documented for proper operation prior to unit startup and during refueling shutdown conditions.

Instrumentation testing can be performed during power operation by closing the isolation valve and opening the test tee located in the instrument line for each pressure switch one at a time. The pressure switch will then actuate at the design set point. Computer alarms are provided in the control room to indicate when each of the three switches (per train) has actuated.