TOLEDO EDISON

LOWELL E. ROE
Vice President
Facilities Development
(419) 259-5242

November 7, 1979

Docket No. 50-346
License No. NPF-3
Serial No. 552

Mr. Darrel G. Eisenhut, Acting Director
Division of Operating Reactors
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Mr. Eisenhut:

Enclosed is Davis-Besse Nuclear Power Station, Unit No. 1 response as requested in your letter dated September 21, 1979, regarding multiple equipment failures and surveillance testing errors.

Yours very truly,

Lowell E. Roe/Ean

LER/TDM/SNB/ljk

Enclosure

1335 047

A001
S
1/1

7911150 332 P

Response to September 21, 1979 Request
Attachment to Toledo Edison Company Letter
Serial No. 552

REQUEST

You and your plant supervisors should review the events described in this letter to determine whether similar errors have occurred or could occur at your facility and whether the potential exists for a problem associated with occurrences that you have not previously considered.

RESPONSE

Toledo Edison personnel have reviewed the events of May 23, 1979 Zion Unit 1 incident. A direct comparison to the safety systems at Davis-Besse Unit 1 is difficult due to the large differences between Westinghouse designs and the Babcock & Wilcox/Bechtel designs incorporated into Davis-Besse Unit 1. At Zion Unit 1, a safety injection signal was initiated by an erroneous test method of inserting a main steam line failure signal. This is required in a Westinghouse unit to assure an adequate shutdown margin is maintained during a main steam line break cooldown of the primary system. Davis-Besse Unit 1 does not require this injection upon a main steam line break and therefore no such safety signal exists at Davis-Besse.

The Westinghouse safeguard system is a combination of Safety Features Actuation System (SFAS), Reactor Protection System (RPS), and Steam and Feedwater Rupture Control System (SFRCS) at Davis-Besse. These systems are independent systems at Davis-Besse with separate electronic components, surveillance tests, and cabinets. A test of the SFRCS cannot directly initiate an actuation signal in any of the SFAS actuated equipment or directly cause an RPS actuation. The same independent relationship is true of the RPS and SFAS.

Davis-Besse Unit 1 has not experienced a trip caused solely by erroneously performed surveillance testing as was the case in the May 23, 1979 event at Zion Unit 1. One unit trip was caused in part by surveillance testing occurred on January 31, 1978 when an SFRCS trip at 67% power resulted in a high pressure RPS trip of the reactor. The SFRCS trip was caused by a spurious half trip in conjunction with an intentional half-trip of the system while performing the monthly surveillance test. The monthly surveillance test has been modified to reduce the likelihood of a recurrence of this problem.

The unit has experienced three unit trips as a result of testing on non-safety related systems. On October 3, 1978, while operating at 73% full power, the second main turbine electro-hydraulic control (EHC) pump was started to investigate the recent reduction in EHC header pressure. A hydraulic perturbation was introduced, tripping the turbine on low EHC pressure. The Integrated Control System (ICS) initiated a reactor power runback at 20% per minute. The increased steam generator pressure and the ICS "cross-limits" rapidly increased feedwater flow, overcooling the Reactor Coolant System (RCS) and causing an RPS reactor trip on low RCS pressure 84 seconds after the turbine trip. The analysis of this trip resulted in a recommended modification to the ICS cross-limits, reducing the amount of feedwater added following any turbine trip.

On February 13, 1979, the reactor was at 88% of full power when a loss of power to startup transformer 02 occurred due to Ohio Edison testing of Beaver Substation. This transformer was being fed from offsite and was supplying power to the 13.8 KV "B" Bus which in turn powers two of the Reactor Coolant Pumps (RCP). The loss of power tripped the RCPs resulting in a reactor trip. The unit is temporarily operating with housepower loads supplied by the startup transformers in order to comply with FSAR commitments. This deficiency will be corrected at the first refueling outage. Ohio Edison has also been informed of the necessity of notifying Toledo Edison prior to the conduct of any relay testing of the sort which initiated this event.

On September 18, 1979, the reactor was at approximately 99% of full power when an instantaneous perturbation in EHC pressure caused a turbine trip and an Anticipatory Reactor Trip System (ARTS) trip of the reactor. The EHC pressure transient was due to a sticking pump pressure controller. General Electric has recommended several design changes to reduce the sensitivity of the trip pressure switch.

Four equipment failures were noted during the May 23, 1979 Zion Unit 1 incident. One deficiency was the failure of one of the four main steam isolation valves (MSIV) to close due to a failure of a pilot valve. The two MSIVs at Davis-Besse Unit 1 are designed with a redundancy in the control circuit so that a single pilot valve failure cannot prevent the MISV from automatically closing upon an SFRCS actuation.

The second failure which occurred at Zion Unit 1 was the failure of the feedwater valve to close, again due to a failed solenoid. Davis-Besse Unit 1 is designed so that both the main feedwater control valves, both main feedwater startup control valves, and both main feedwater stop valves close upon an SFRCS actuation. The controls for these valves are independent so that a failure of any one solenoid cannot prevent the isolation of the line from an SFRCS signal.

The third failure which occurred at Zion Unit 1 was a failure of one of the main steam line safety valves to reseat. Davis-Besse Unit 1 has experienced approximately 200 individual valve actuations without the occurrence of a stuck open valve. The valve vendor was contacted and has verified no difficulties with safety valves failing to reseat has been experienced in the safety valves of the type supplied to Davis-Besse Unit 1.

The final failure noted in the Zion Unit 1 occurrence was the failure of the Auxiliary Feed Pump (AFP) due to an improperly adjusted governor. Although Davis-Besse Unit 1 has experienced difficulties in AFP speed control in the past, design changes to the speed control circuit have corrected the deficiencies and greatly increased the reliability of the system. No AFP speed control difficulties have occurred in the last twenty-two months. The pumps are verified operable on a monthly basis by surveillance testing.

REQUEST

In addition, it is requested that management policies and procedures be reviewed and strengthened as necessary to assure that multiple equipment failures in safety-related systems will be vigorously pursued and analyzed to identify potential failure modes not previously considered that could lead to a significant reduction in the ability of safety systems to function as required.

RESPONSE

At Davis-Besse Unit 1 every unit trip associated with a protective system or safeguard system actuation is presently investigated by the Technical Section and a report is prepared for review by the corporate office, the plant operating staff, and station management. Unresolved items have been and will continue to be given the highest priority. Multiple equipment failures in safety-related systems are vigorously pursued and analyzed to identify failure modes not previously considered that could lead to a significant reduction in the ability of safety systems to function as required. This commitment is integral to our compliance with Criterion XVI of 10 CFR 50, Appendix B which requires that for significant conditions adverse to quality, measures shall be provided to assure that the cause of the condition is determined and corrective action is taken to preclude repetition.

Station Administrative Procedure AD 1807.00, "Control of Conditions Adverse to Quality" provides a format to meet this nuclear quality assurance requirement. A significant improvement has been afforded this procedure recently by the institution of Licensee Event Report Investigating Committees which promptly investigate reportable occurrences with particular emphasis upon the finding of root causes, and examining additional potential problems. This committee allows responsible senior plant supervision and members from various sections to investigate the event in detail and has enhanced the station's ability to provide a comprehensive investigation of problems related to the safe operation of the unit.

The formation of a new corporate Licensee Event Report Review Committee now provides in-depth assurance of the adequacy of problem resolution and additional consideration into the determination of potential defects which could lead to an impaired ability of safety-related systems to function as designed.

These groups will augment the station and corporate engineering staffs' continued effort to analyze and rectify potential deficiencies. To date, the new program has improved the quality of followup corrective action involving reportable events, and management emphasis will continue to be persistently placed in this area.

REQUEST

Finally, you are requested to review your engineered safety system surveillance procedures to determine whether appropriate cautions are included and to ensure that plant operators and supervisors are aware of the importance of avoiding challenges to the protective features of your facility.

RESPONSE

All monthly surveillance procedures for the Safety Features Actuation System (SFAS), Reactor Protection System (RPS), and Steam and Feedwater Rupture Control System (SFRCS) have been reviewed by Toledo Edison personnel. The following is a summary of the administrative and procedural controls present in the test methods.

1. Safety Features Actuation System

   The Safety Features Actuation System provides four independent channels arranged in a two-out-of-four logic to provide for containment isolation and to initiate the operation of safety related equipment in the event of a loss of coolant accident.

   The four SFAS channels are located in individually locked cabinets with independent locks. Administrative controls assure there is no more than one channel key issued at a time to prevent an inadvertent actuation by the testing of two channels simultaneously.

   Within each SFAS channel there is a test bypass function switch which is selected to any one of the four input parameters. When the bypass switch is selected to a particular input, it removes the channel under test from the trip sequence and prevents the SFAS actuation from the circuit being tested. The procedure is carefully detailed to assure test signals are not induced to a parameter that was not selected by the test bypass switch. Only one trip signal would be generated if the trip signal was induced on a parameter which was not bypassed, thereby not causing an erroneous actuation of the SFAS.

   The procedures also stipulate performing testing on one channel at a time and verifies erroneous trips do not exist on other channels prior to proceeding with the normal testing.

2. Reactor Protection System

   The Reactor Protection System design incorporates four independent logic channels to provide trip signals to the Control Rod Drive Control System and utilizes a two-out-of-four trip logic during normal system operation.

The four RPS channels are located in individually locked cabinets with independent key locks. Sufficient administrative controls exist to prevent the issuance of more than one channel key at a time during testing or maintenance. One channel at a time of the RPS can be bypassed for testing, preventing the tripping of the channel under test even if an improper test signal is induced.

The procedure presently requires verification that the master trip module indicates no erroneous trips prior to proceeding with the normal testing. Further precautions will be added to the RPS procedure to assure the test personnel are aware of the importance of appropriate cautions. This procedure modification is expected to be completed by December 1, 1979.

3. Steam and Feedwater Rupture Control System

The Steam and Feedwater Rupture Control System is designed with four independent channels which are configured into two trip channels using a one half (1/2) logic for a half trip and a 2/2 logic for a full trip. Full actuation of the system provides for selected isolation of the steam generator(s) if required and initiation of auxiliary feedwater.

Although only one of the two channel keys are issued at a time, this does not in itself prevent a partial actuation of equipment from the tripping of one channel. Prevention of inadvertent trips is provided by:

(a) Proper procedure precautions have been incorporated to insure no trips exist prior to testing that could cause an inadvertent actuation.

(b) System design modifications have been completed to prevent spurious unwarranted trips from occurring. This prevents an accidental full actuation signal from being generated by one channel in test simultaneous to a spurious trip of the opposite channel.

All protective systems are designed for redundancy, diversity, and test ability per IEEE Standard 279-1968/1971. This provides for isolation of all signals leaving or entering the systems by isolation amplifiers or relay contacts so that two or more protective channels cannot interact through the cross-coupling or faulting of related signal lines. Separability insures that each RPS, SFAS, and SFRCS channel is powered from a different essential bus so that power supply faults can affect only one channel at a time. Separability also ensures that redundant sensors in each Class IE channel and their connections to the process system have been sufficiently separated to ensure that the functional capability of the protective system has been maintained despite a single failure. Multiple failures are not addressed, however, proper procedural and

administrative precautions do exist to preclude additional inadvertent actuations and challenges to the protective systems from testing operations.

The monthly surveillance test procedures associated with these systems have been reviewed to insure that only one channel is tested at a time and that adequate cautions exist within two procedures to insure that inadvertent equipment actuations do not result during testing due to variable plant conditions or equipment status. Detailed expected indications must be verified within the procedures, with precautions to notify the Shift Foreman and Instrument and Control Engineer if inconsistencies are observed. These and other precautions mitigate the potential for component failures, or procedural errors to affect system testing by insuring at all times proper test and output indications are confirmed before proceeding to subsequent steps.

As in the case of the SFRCS, known design inadequacies have been corrected to provide improved system operation, and such an effort will continue.

Present technical specifications do require the tripping of an inoperable channel (in both SFAS and RPS) which reduces the logic to a one out of three actuation. This requirement forces the unit into a single failure (or single error) actuation of the system. Toledo Edison feels this policy is worthy of additional review and should allow the bypassing of an input verified to be erroneous.

The review with the exceptions noted has verified sufficient administrative and design features exist to reduce inadvertent equipment actuations and challenges to the protective features to a minimum.