THREE MILE ISLAND NUCLEAR STATION, UNIT 1, DOCKET NO. 50-289

SAFETY EVALUATION

PROTECTION, CONTROL AND EMERGENCY POWER SYSTEMS

Protection and Control Systems

General

The Proposed IEEE Criteria for Nuclear Power Plant Protection Systems (IEEE No. 279) and the Commission's General Design Criteria served, where applicable, as the bases for judging the adequacy of the protection system.

The protection system design is substantially the same as that for Oconee Unit No. 1. There is a minor difference relating to the separation of control and protection functions which is discussed later in this report. Since the basic protection system design was reviewed extensively during the Oconee licensing process, our TMI-1 review has emphasized those items which are unique to this station (including design variations by the architect-engineer within the constraints of the basic design), for which new information has been received, or which have been generic concerns.

Our review has included a detailed study of the following protection system schematic diagrams: (1) Reactor Trip, (2) High Pressure Injection, (3) Low Pressure Injection, (4) Containment Spray, (5) Fan Cooler, and (6) Contained Isolation.

The site was visited on March 9, 1972 for the purpose of reviewing the installed protection, control and emergency power systems.

Schematic Diagrams

Our review of the Reactor Trip (Scram) system schematics indicated that, with one exception, the system satisfied IEEE-279. The exception was the use of administratively controlled "Dummy Modules" for bypassing the individual instrument logic channels for maintenance and testing purposes. Our concern was that administrative control was not adequate to ensure that the system protective function would not be inadvertently negated. The applicant agreed to remove these modules from the design. The matter has been satisfactorily resolved.

Our review of the engineered safety feature schematics indicates that, in addition to being properly designed in split-bus arrangements and otherwise satisfying IEEE-279 and the GDC, several circuits have an on-line testing capability. For example, the High Pressure Injection System has test provisions for initiating the pumps but not the valves. The valves can be exercised independently of the pumps.

All protection system circuits can be completely tested when the reactor is shut down.

There is one exception to the split-bus design: one containment ventilation fan automatically swings between two redundant a-c emergency

buses in order to satisfy the single failure criterion under non-accident conditions. The swing feature is bypassed under accident conditions. We have reviewed the design and concur with the applicant that no single failure will permit the swing bus to interconnect the two redundant and non-synchronized emergency buses or otherwise precipitate a loss of all onsite power. While we would prefer a system which satisfies Safety Guide 6, we believe that this design, inasmuch as it satisfies the single failure criterion, is acceptable for this plant and that backfit is not required.

Our review of the rod control system schematics indicates that a single electrical failure could permit an extra rod group to be inadvertently withdrawn. We concur with the applicant that such a transient would be successfully terminated by the protection system. We believe that this aspect of the design is acceptable.

A design feature of the rod control system provides the capability to patch the various rods into various control stations. The purpose of this feature is to permit the assignment of rods to rod groups as desired. This feature, however, creates the administrative problem of ensuring that the intended rod is, in fact, controlled by the intended station. The problem arises from the fact that a "wrong" rod will give indications at the continuous position indicator which are indistinguishable from those which would be given by the "correct" rod.

There are, however, coarse position indicators (0-25%-50%-75%-100%) for each rod which are independent of the patching circuits; i.e., the coarse indicators are hard-wired. Whenever any patching is accomplished, these lights can be used for comparison with the continuous position indicators at the control stations to ensure that the rods are connected properly.

We believe the patching scheme can be safely implemented provided there are stringent administrative procedures to guard against errors. These procedures will be included in the technical specifications which are now under review.

Apart from the one serious concern relating to protection system bypasses, which has been satisfactorily resolved, our review of the protection system schematic diagrams uncovered no deficiencies.

Qualification Testing

a. LOCA Conditions

Protection system instruments which would be subjected to a LOCA or steam line break accident environment are designed to withstand the environment for the length of time they would be required to operate under these conditions. Design conditions range upwards to 60 psig, 100% humidity and a dose of 10,000 R.

Qualification tests under simulated LOCA and steam line break conditions have been performed and are analyzed in the B&W topical report "Qualification Testing of Protection System Instrumentation (BAW-10003)" Rev. 1. We have reviewed the applicant's submittals and determined that the protection system components have been properly qualified, by test, for the postulated LOCA environment.

LOCA qualification tests were performed on the motor units for the Reactor Building fan assemblies. These tests were performed in accordance with the "IEEE Proposed Guide for Qualification Tests for Class IE Motors Installed Within the Containment of Nuclear Fueled Generating Stations," NSG/MCS/SC2-A, dated June 1969. This proposed guide was ultimately published as "IEEE Trial-Use Guide for Type Tests of Continuous-Duty Class I Motors Installed Inside the Containment of Nuclear Power Generating Stations, IEEE Std 334-1971." The proposed guide and IEEE Std 334-1971 are substantially the same in terms of technical content.

The fan motors are water-cooled, totally enclosed, two-speed induction motors. Our review of the applicant's test results and analyses indicates that the fan motor units are adequately qualified for the LOCA (steam, pressure, chemical and radiation) environment.

Representative samples of pre-aged cables were tested under high pressure, temperature and humidity conditions. The cables were pre-aged for forty years of radiation and temperature prior to testing. Radiation dose levels consistent with extended accident conditions were not addressed for those cables that power long-term accident loads. No specific details concerning the cable tests have been submitted; e.g., the number and kind of LOCA transients, duration of tests, test results, etc.

Until suitable information (including postulated accident dose levels) is received and evaluated, we must withhold judgment concerning the acceptability of the cables to be used within containment.

A typical production valve and its actuator used for containment isolation were also tested under simulated LOCA conditions. We have reviewed the information submitted by the applicant and determined that the qualification test was adequate.

Cable Installation

We have reviewed the applicant's criteria with respect to the installation of redundant power, control and protection system cables and concur with the criteria.

The cable system was reviewed during the site visit and two deficiencies were uncovered. The cabling between the control room and the cable spreading room, which was in the process of being installed, did not appear to be governed by any quality assurance procedures relating to separation of redundant wiring. This matter was referred to RO for resolution.

The site review also uncovered an apparent deficiency in the color coding scheme for ensuring separation of redundant engineered safety feature circuits. Several ESF circuits involve two-out-of-three logic schemes which require three separate cable runs to ensure independence. None of the ESF cable tray or conduit systems were identified by three distinct colors. This matter was referred to RO to ensure that these cables are properly separated.

Separation of Control and Protection Systems

At Oconee, the control system inputs are derived from channels that are within the protection system or independent of the protection system. At TMI-1, the input can be derived only from protection system channels; however, only one channel at a time can be selected for concurrent protection-control system functions.

The safety implications of this design difference are not significant.

In all cases, the control systems are isolated from the protection system and, in addition, any failure of a common element (e.g., a sensor) would leave intact a redundant protection system as required by Section 4.7 of IEEE-279.

We believe that the design, since it conforms to Section 4.7 of IEEE-279, provides adequate defense against random failures. Common mode failures which affect the interaction of control and protection systems are being reviewed on a generic basis.

Emergency Power System

General

The Commission's General Design Criteria, IEEE-308, and Safety Guides 6 and 9 served, where applicable, as the bases for judging the adequacy of the emergency power system.

Offsite Emergency Power System

Power is brought to the switchyard over two divergent rights-of-way. The switchyard breakers are arranged in a breaker-and-a-half configuration. Each breaker has two trip coils (for fault clearing) controlled by redundant circuits. Power from the switchyard is fed to the plant via two startup transformers.

Stability studies show that the grid can withstand the sudden loss of the TMI-1 generator or the most critical unit on the grid.

We have concluded that the offsite emergency power system satisfies the applicable criteria and is acceptable.

Onsite Emergency Power System

With the exception of one swing bus at the 480 volt level, discussed previously, the a-c portion of the onsite system is redundant and split throughout in accordance with Safety Guide 6. Maximum diesel generator loading in the event of an accident is 2513 kW which is below the 2000 hour rating of the diesels in accordance with Safety Guide 9.

The diesels are located in separate rooms and are individually started by loss of voltage at their respective buses. The offsite supply breakers to each emergency bus are respectively opened (in response to undervoltage) by control circuits energized from the d-c subsystem assigned to that bus. The starting of a diesel is in no way conditioned by operation of the other.

There are two station batteries located in separate, adjacent rooms. With the exception of a single swing bus, the d-c system is also split throughout and is compatible with the split a-c system. Although the swing bus does not conform to Safety Guide 6, our review indicates that the associated circuits are adequately fused to prevent a single fault from disabling both d-c systems. Further, the automatic swing feature is bypassed under accident conditions. For these reasons, we believe

that the design is adequate for this plant and that backfit is not required.

The batteries are located in separate rooms. The rooms are ventilated by redundant supply and exhaust fans which share a common duct external to the rooms. The fans are energized from the emergency a-c buses. One deficiency was uncovered during the site visit: lighting fixtures of unknown seismic integrity were observed to be suspended directly over both batteries. This matter is outside of our review scope and has been referred to Licensing for resolution.

Apart from this one concern, we have concluded that the design of the onsite emergency power system is acceptable.