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 our bases for judging the adequacy of the protection system.

The protection system design is substantially the same 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), or 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 Coolers, and (6) Contained Isolation. It is presently anticipated that the site visit by Electrical Systems Branch staff members will take place in September.

7910170810

1450 256

Schematic Diagrams

Our review of the Reactor Trip (Scram) system schematics indicated that, with one possible exception, the system satisfied IEEE-279. The exception relates to the lack of information available to us concerning the bypassing of instrument channels during power operation. We understand that there are two key-operated bypass switches at each protection channel. The adequacy of the administrative control over these bypasses, including suitable control room indication, is not clear to us at present. We are continuing to pursue this matter with the applicant and will report to the Committee later.

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, the circuits have a high degree of on-line testability. This results from the fact that functions which cannot be simultaneously accomplished on-line are controlled by separate relays which can be tripped individually. 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.

There is one exception to the split-bus design: one containment ventilation fan must swing between two redundant a-c emergency buses in order to satisfy the single failure criterion. 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. 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 to the operator which are indistinguishable from those which would be given by the "correct rod". There are 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 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 our one concern relating to protection system bypasses, our review of the protection system schematic diagrams uncovered no other 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)". Our review of this document is incomplete at this time. We will report the results of our review to the Committee later.

b. Seismic Conditions

The protection system instruments are designed to function normally during and after the design basis earthquake.

1450 259

Seismic qualification tests have been conducted and are also analyzed in BAW-10003. These analyses are being reviewed.

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. We will review the installed system during a site visit.

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.

1450 260

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 are asking the applicant to determine if a turbine trip followed by a single failure in the switchyard (e.g., bus, breaker, battery) will cause the loss of all access to offsite power. Our concern is that the single failure might require isolation of the entire switchyard by external fault-clearing devices in order to isolate the monitoring generator.

Apart from this one concern which we expect to discuss with the Committee later, we conclude that the offsite emergency power system satisfies the applicable criteria and is acceptable.

1450 261

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. For this reason, 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.

We conclude the design of the onsite emergency power system is acceptable. We will review the installed system during our forthcoming site visit.

MAY 1 5 1971

POOR ORIGINAL

P. A. Morris, Director, Division of Reactor Licensing

SAFETY EVALUATION, PROTECTION, CONTROL AND EMERGENCY ~~POWER SYSTEMS~~, THREE MILE ISLAND NUCLEAR STATION, UNIT 1; DOCKET NO. 50-289

The safety evaluation relating to the protection, control, and emergency power systems for the Three Mile Island Nuclear Station, Unit 1, is enclosed.

Original Signed By
E. G. Case
E. G. Case, Director
Division of Reactor Standards

Enclosure:
Safety Evaluation

cc w/encl:
S. Hanauer, DR
R. DeYoung, DRL
R. Boyd, DRL
D. Skovholt, DRL
C. Long, DRL
V. Moore, DRS
D. Ross, DRL
D. Sullivan, DRS

Distr:
DR RF
DRS RF
ESB RF

1450 263

CRESS T64, R1 ebk						
OFFICE ▶	DRS	DIR:DRS	DRS:ESB			
SURNAME ▶	D Sullivan	EG Case	MOORE			
DATE ▶	5/13/71	5/13/71	5/14/71			

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

U. S. GOVERNMENT PRINTING OFFICE 1971-416-463