UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

ENCLOSURE 1

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

OF DECEMBER 3, 1986 EVENT

RELATED TO THE MSIV ACTUATION LOGIC DESIGN

AT NINE MILE POINT, UNIT 2

DOCKET NO. 50-410

1.0 INTRODUCTION

The main steam isolation valve (MSIV) actuator control system for Nine Mile Point, Unit 2 (NMP-2) was modified to compensate for deficiencies found within the mechanical portion of the original MSIV actuator design. The original actuator design consisted of a mechanical latching mechanism to hold the valve open and two normally-energized solenoid operated spring plungers to release the mechanism and permit spring closure of the valve. Each solenoid was powered from separate, independent Uninterruptible Power Supply (UPS) systems and it took the deenergization of both solenoid spring plungers to initiate closure of the associated MSIV (i.e., disengage the mechanical latch). Testing of the original design revealed that in some cases the force produced by the solenoid operated spring plungers was inadequate to trip the mechanical latch.

Subsequently, the licensee decided to eliminate the use of the mechanical latch trip system described above and to utilize the hydraulic system, originally intended only to open the MSIVs, to maintain the MSIVs in the open position. This re-design proposes using the solenoid operated valves (SOVs), which are part of the original hydraulic system. These SOVs will be normally energized to keep the solenoid valves closed, thereby maintaining the hydraulic pressure to keep the MSIVs open. Deenergization of any one of the SOVs will cause rapid closure (release of hydraulic pressure) of the associated MSIV. In an attempt to enhance MSIV availability and to be consistent with the original MSIV actuator system design, the licensee has chosen to provide power to each SOV from either of the two independent UPS systems through auctioneering circuitry in order to assure that loss of one power supply system will not deenergize (open) either SOV. However, during testing of the new actuation control system, an event occurred on December 3, 1986, (described below) which caused a complete loss of power supplies to both divisions of the reactor protection system trip channels resulting in a full scram of the reactor. The staff met with the licensee on December 18, 1986, to obtain information on what actually caused the event, held further discussion on the proposed logic modification by telecon on December 22, 1986, and met again with the licensee on January 6, 1987 to discuss the interactions of RPS logic and the proposed MSIV logic.

2.0 EVALUATION

The RPS Trip channels and MSIV actuation logic trip channels, including the

hydraulic SOVs, are powered by redundant UPS systems. These systems are partially qualified as Class 1E and Category I to ensure reliability of the RPS scram trip function. FSAR Section 8.3.1.1.3 indicates that the RPS power supply system that powers the RPS logic system is designed in accordance with the requirements of IEEE Standard-279 and General Design Criterion (GDC) 21. Therefore, it is the staff's understanding that the NMP-2 design basis includes the implementation of the provisions of Regulatory Guide 1.75 for the Class 1E portion of the UPS system so that the reliability of the RPS would not be jeopardized even after assuming a single failure. The original MSIV actuation logic design, which utilized the independently powered solenoid spring plungers, met this design basis. However, the modified actuator control system allows the automatic transfer from one UPS bus to its redundant counterpart for a single load (SOV), thus creating a potential for paralleling of the redundant power supply systems of the RPS trip channels. The December 3, 1986 event resulted in a relay contact race within the Class 1E portion of the design which created an electrical system transient that caused the redundant RPS Class 1E power supply systems to be interrupted and scrammed the reactor. The licensee has proposed to correct the relay contact race problem by utilizing additional contacts of the same relay. During discussions on this latest proposed design change, the staff advised the licensee that a single failure could still result in the interconnection (paralleling) of the redundant Class 1E portions of the RPS power supply system and, thus, challenge the independence of redundant trip channels of the RPS. These latest design changes rely on the Class 1E Electric Protective Assemblies (EPAs) to protect against events (electric transients) developing from interactions within the protection system as well as to protect against abnormal conditions originating only from the nonsafety-related power sources (external to the Class 1E portion of the design), which was the original design basis.

3.0 CONCLUSION

Based on its review of this issue, the staff concludes that the design modifications to enhance MSIV availability are unacceptable. The proposed design change would potentially decrease reliability of the RPS in that a single failure (relay and associated contacts) can result in the interconnection between the redundant RPS Class 1E power supply systems, thereby inducing interactions between the redundant channels of the RPS. Therefore, the staff finds that the design, as currently modified, does not comply with IEEE Standard 279 channel independence requirements (i.e., the protection channels shall be independent and physically separated to accomplish decoupling of effects of electrical transients). Further, unnecessary challenges to the RPS could significantly degrade the high functional reliability of the protection system which is required by GDC 21.