UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REACTOR REGULATION
WASHINGTON, D.C. 20555-0001

February 14, 2005

NRC INFORMATION NOTICE 2005-04: SINGLE-FAILURE AND FIRE VULNERABILITY OF REDUNDANT ELECTRICAL SAFETY BUSES

ADDRESSEES

All holders of operating licenses for nuclear reactors, except those who have permanently ceased operations and have certified that fuel has been permanently removed from the reactor vessel.

PURPOSE

The U.S. Nuclear Regulatory Commission (NRC) is issuing this information notice to inform addressees of a potential single-failure and fire vulnerability whereby a circuit failure could result in bus lockouts and prevent the reenergization of the redundant electrical safety buses. It is expected that recipients will review the information for applicability to their facilities and consider appropriate actions to avoid similar problems. However, suggestions contained in this information notice are not NRC requirements; therefore, no specific action or written response is required.

DESCRIPTION OF CIRCUMSTANCES

On January 27, 2005, during a triennial fire protection inspection of the Crystal River nuclear station, NRC inspectors discovered an electrical protection and metering circuit which if damaged, could electrically lock out redundant safety buses and prevent reenergization of the buses both from offsite power sources and emergency diesel generators (EDGs).

The power sources for the safety buses generally consist of two offsite power supplies, both of which are designed to supply power to each of the safety buses. The normal bus alignment has one offsite power supply selected as the source for each safety bus. Each safety bus also has one EDG as a standby power source. The electrical protection and metering system uses current transformers (CTs) for measuring power consumption and sensing overloads and faulted conditions. At Crystal River, the electrical protection and metering circuit for each offsite power supply included three CTs at the feeder breaker to each safety bus, phase overcurrent relays, and ground overcurrent relays, all connected in a basic residual scheme. The circuit also included one watt-hour meter which would sum the power to both safety busses. This interconnection of a protection and metering circuit between two safety busses was identified by the inspectors as a common-mode failure vulnerability. A failure on this interconnected circuit (e.g., a fire-induced cable fault or watt-hour meter failure) would be interpreted by the protection system as an electrical bus fault on both safety busses. Consequently, the relay logic would lock out both redundant safety buses and prevent reenergization from any power source.

ML050400090

The licensee has modified the wiring in the overcurrent protection circuits to align each monitoring circuit to one safety bus and to disconnect the watt-hour meters. In this corrected configuration, each circuit is contained within one switchgear, a single fault will affect only one safety bus, and a fire in any area (e.g., at the watt-hour meters in the main control room) will not affect safety busses that are relied upon for safe shutdown.

BACKGROUND

The design function (to prevent single- failure vulnerabilities) is implemented through train-specific metering, monitoring, and protection systems to limit the probability of worst case failures to a train. Whenever a signal is needed to the redundant train, the signal is electrically isolated (i.e., any potential failure or its deleterious effects cannot be transmitted to the redundant train).

The redundant safety buses are expected to be fully independent (i.e., neither component failure, degradation of equipment, or electrical faults could disable both trains). NRC regulations in Title 10, of the *Code of Federal Regulations* (CFR) Part 50.55a(h)(2), requires protection systems to meet IEEE Std 279 -1971 "Criteria for Protection Systems for Nuclear Power Generating Stations." This standard requires all electric and mechanical components (e.g., from sensors to actuation devices) to be free from single failure vulnerability. That is, no single failure in the protection system shall prevent proper protective actions at the system level.

General Design Criterion (GDC)17, of 10 CFR Part 50 Appendix A, states that "The onsite electric power supplies...and the onsite electric distribution system... shall have sufficient independence [and] redundancy ....to perform their safety functions assuming a single failure." There may be other plant-specific commitments for keeping the plant configuration free of single-failure vulnerability.

DISCUSSION

The design deficiency identified at Crystal River had a protection scheme that used CTs for monitoring and metering power flow. The CTs installed on power feeders to redundant safety buses were electrically connected to generate a selective tripping scheme to isolate overcurrent and ground fault conditions on the bus. This design is economical but results in a common-mode failure vulnerability disabling two redundant trains of safety buses. Further, the CT outputs from redundant safety buses were also connected to the same watt-hour meter, resulting in the same vulnerability to common-mode failure.

The significance of such a vulnerability is that the failure of redundant buses generally disables most of the accident mitigation/emergency core cooling systems, except the steam-driven systems actuated by DC power. Such electrical failures cannot be isolated with a reasonable chance of system recovery without expert help because of the interdependent electrical protection system. In most cases, manually closing the breaker will result in a prompt trip. This is because the logic is designed to prevent such operations when actual fault conditions persist.

Similar problems could exist in the buses that supply related plant pumping systems (e.g., reactor coolant pumps, circulating water pumps, service water pumps), where a single failure could disable the full system of pumps connected to different buses.

Similar common-mode failure vulnerabilities were identified at Quad Cities, Dresden, LaSalle, Prairie Island, and Monticello.

GENERIC IMPLICATIONS

After reviewing the events at the six sites (10 units), the staff concludes that such deficiencies are potentially wide-spread with varying levels of risk significance depending on plant-specific, unique design configurations.

CONTACT

This information notice requires no specific action or written response. Please direct any questions about this matter to the technical contact listed below or the appropriate Office of Nuclear Reactor Regulation (NRR) project manager.

/RA/
Patrick L. Hiland, Chief
Reactor Operations Branch
Division of Inspection Program Management
Office of Nuclear Reactor Regulation

Technical Contact: Thomas Koshy, NRR/EEIB
301-415-1176
E-mail: txk@nrc.gov

Note: NRC generic communications may be found on the NRC public Website, http://www.nrc.gov, under Electronic Reading Room/Document Collections.