CONF-850206--8

Reliability Assurance Program for Operational Emergency AC Power Systems*

CONF-850206--8

DE85 002554

J. B. Heineman, W. A. Ragland, and C. J. Mueller

Summary

A comprehensive review of emergency AC power systems in nuclear generating plants (the vast majority of these plants contain redundant diesel generator systems) delineates several operational areas that can be improved by instituting a reliability assurance program (RAP), which (1) initially upgrades the diesel generator performance (if required) and (2) provides for ongoing monitoring and maintenance based upon alert levels. The alert levels are based upon a two-tiered structure, (1) a degraded performance level which requires maintenance/repairs to restore the diesel performance level to a predetermined baseline, and (2) a more severely degraded performance level which challenges the plant safety, based upon a computed increase in unavailability such that the fractional contribution to the probability for station blackout is increased beyond an acceptable level.

The program described herein is a subset of an overall reliability program development for the assurance of nuclear power plant safety; this more general development is an ongoing effort which evolved from a comprehensive review (reference 1) of risk and reliability engineering techniques from nuclear and other high technology industries.

Station blackout is defined as the loss of all AC power at a nuclear power plant. Station blackout reduces the ability to provide cooling to the

---

* This work was performed under the auspices of the U.S. Nuclear Regulatory Commission.

reactor core by disabling the normal cooling systems and may also disable part of the emergency cooling systems. For this reason station blackout has been classified as an unresolved safety issue by the NRC (USI-44). When the reactor is operating, there are three supplies of AC power to the plant: unit generator, offsite power grid, and onsite emergency AC power system. During reactor shutdown only the latter two supplies are available. In the event of loss of offsite power, the reactor and unit generator may also shutdown due to inability to follow load. Under these conditions, the emergency AC power system is the sole source of AC power.

Although this study focuses on a specific unit as a "case study", the strategy and procedures described should be generally applicable to any nuclear plant diesel generator (DG) system. Based upon a review of the current station blackout literature and existing PRAs, a specific nuclear unit was selected as a case study for application of the approach herein. The criteria for selection are (1) the unit employs a system produced by a major (i.e., widely employed) diesel manufacturer; (2) the operating strategy for redundancy should be widely employed but of low complexity; (3) the unit has an existing PRA. More specifically, with respect to the parameters pertinent to reliability analysis, the unit has the following characteristics:

(1) the unit provides 3 diesel generators solely dedicated to the unit during offsite power failure;

(2) the generators employ a 1/3 operating strategy;

(3) from the existing PRA for the plant, station blackout constitutes a significant (> 20% prediction) contribution to the probability of core melt.

A detailed description of diesel generator performance criteria and associated alert levels is provided in the full paper. An outline of the approach is provided herein. The analytical procedure for determining alert levels may proceed using a specific plant data base or using a generic (industry-wide) data base, or some combination of both, dependent upon (1) the current performance of the specific plant diesel and (2) the modeling used in calculating the diesel generator availability.

For the purposes of this study, the following strategy and specific data base values are used:

(1) The specific plant value of diesel generator failure rate on demand from periodic testing is determined from available test data.

(2) The generic value of DG failure rate on demand is selected (e.g., from LER data in reference 2). This serves as the baseline value for the performance-related (i.e., nonsafety) alert level.

(3) During the implementation and integration phase of the RAP, the value from (2) is used to determine the necessity or non-necessity of upgrading the current DG system.

(4) A reliability monitoring program based upon a "moving average" (i.e., trend analysis) of failure rate (or availability) is established.

(5) If the trend analysis indicates a value dropping below the baseline alert level established in (2), then the RAP institutes appropriate maintenance/repair procedures.

(6) The value of diesel generator failure rate on demand for the specific plant is determined from the PRA or other available data. This value and consideration of additional overall plant risk factors related to specific safety issues are used to determine the alert level value for a potentially severely degraded performance level (i.e., safety challenge).

It should be emphasized that if this value is too conservative (e.g., it may match the same value determined in (1)), then some higher value can be selected with a concommitant increase in the importance to safety. Alternatively, the performance-related alert level and the safety-related alert level can be identical. In any case, this alert level triggers RAP procedures designed to rapidly improve DG performance.

It should be noted that there is the assumption in the above strategy that none of the values determined exceed any of the current NRC requirements for maximum DG failure rates in periodic testing.

In order to partially substantiate the analysis for this study, a diesel generator fault tree was devised based upon the nine diesel generator subsystems and their importance levels found in reference 2. The results of the DG failure rate analysis (i.e., availability) compare favorably with those derived from industry-wide data bases.

The key to successful implementation of the RAP is the monitoring program. The major elements include:

(1) Trend analysis of periodic testing data (system failure rate data).

(2) Trend analysis of subsystem parameters (pressures, temperatures, oil levels, fuel feed rates, chemical analyses, measures of wear and corrosion, etc.).

(3) Regular preventative maintenance and inspection procedures.

Note that (1) is related to the overall DG performance as determined by periodic testing of the entire system. The results of this testing as processed by the monitoring system may trigger an alert level. Elements (2) and (3), however, may also trigger an alert level at points in time between periodic testing, since input to the monitoring program from (2) and (3) may indicate that sufficiently degraded DG performance would occur if the unit were tested or called upon to provide emergency AC power.

References:

(1) NUREG/CR-3932, ANL-84-34, "Benchmark Description of Current Regulatory Requirements and Practices in Nuclear Safety and Reliability Assurance", S. L. Halverson, W. A. Bezella, I. Charak, and C. J. Mueller, prepared for the Office of Nuclear Regulatory Research, USNRC, August, 1984.

(2) "Diesel General Reliability at Nuclear Power Plants: Data and Preliminary Analysis", NP-2433, Research Project 1233-1, by SAI for EPRI, Interim Report, June, 1982.