SAFETY GUIDE 6

INDEPENDENCE BETWEEN REDUNDANT STANDBY (ONSITE) POWER SOURCES AND BETWEEN THEIR DISTRIBUTION SYSTEMS

A. Introduction

General Design Criterion 17 requires that onsite electrical power systems have sufficient independence to perform their safety functions assuming a single failure. This safety guide describes an acceptable degree of independence between redundant standby (onsite) power sources and between their distribution systems.

This guide does not address the suitability of nearby hydroelectric, nuclear, or fossil units as standby power sources at multiple-unit sites. This matter will be evaluated on an individual case basis.

B. Definitions

Preferred Power System: The offsite external commercial power system.

Standby Power System: Those onsite power sources and their distribution equipment provided to energize devices essential to safety and capable of operation independently of the preferred power system.

Standby Power Source: An electrical generating unit and all necessary auxiliaries, usually a diesel generator set, which is part of the standby power system.

Load Group: An arrangement of buses, transformers, switching equipment, loads, etc., fed from the same power source.

C. Discussion

There is evidence based on operating experience and analytical considerations that the parallel operation of standby power sources renders them vulnerable to common mode failures. Current designs are therefore based on the concept of independent, redundant load groups. In these designs, the standby power source for one load group is never automatically interconnected under accident conditions with the standby power source of a redundant counterpart.

There can also be compromises of independence resulting from automatic bus ties (both a-c and d-c) which connect the loads of one load group to the power source of another in the event the power source of the first load group has failed. The slightly improved defense against random failures achieved by these bus ties is more than offset by the additional vulnerability to common mode failures which they create.

A special case of the foregoing is the bus that is automatically transferred to one or the other of two redundant standby power sources; this is commonly referred to as a swing bus. This arrangement also compromises the independence of redundant power sources and their load groups while adding little to the defense against random single failures.

The inclusion of a swing bus in an otherwise well designed system often results from an incompatibility between the number of standby power sources (whether a-c or d-c) and the number of redundant load groups. For example, an engineered safety feature system design which depends on the operation of at least two of three electrically driven pumps and which derives power from either of two redundant standby power sources must provide for the swinging of one of the three pump motors in order to meet the single failure criterion. A compatible design, such as one based on three power sources, would not utilize the swing feature.

The necessity for a swing bus can also result from an incompatibility between the a-c and d-c power sources themselves. An example would be a three diesel generator, three bus system utilizing d-c control circuits. If only two

d-c sources are provided, the switching of diesel generator control circuits between the d-c sources becomes necessary in order to provide the necessary redundancy. Again, a compatible design such as one based on three d-c sources, one for each generator, would not utilize a swing bus.

A diesel generator that swings between the load groups of different units at a multiple unit site is not an example of the foregoing since such load groups are not redundant to each other.

D. Regulatory Position

1. The electrically powered safety loads (a-c and d-c) should be separated into redundant load groups such that loss of any one group will not prevent the minimum safety functions from being performed.
2. Each a-c load group should have a connection to the preferred (offsite) power source and to a standby (onsite) power source (usually a single diesel generator). The standby power source should have no automatic connection to any other redundant load group. At multiple nuclear unit sites, the standby power source for one load group may have an automatic connection to a load group of a different unit. A preferred power source bus, however, may serve redundant load groups.
3. Each d-c load group should be energized by a battery and battery charger. The battery-charger combination should have no automatic connection to any other redundant d-c load group.
4. When operating from the standby sources, redundant load groups and the redundant standby sources should be independent of each other at least to the following extent:
   a. The standby source of one load group should not be automatically paralleled with the standby source of another load group under accident conditions;
   b. No provisions should exist for automatically connecting one load group to another load group;
   c. No provisions should exist for automatically transferring loads between redundant power sources;
   d. If means exist for manually connecting redundant load groups together, at least one interlock should be provided to prevent an operator error that would parallel their standby power sources.
5. A single generator driven by a single prime mover is acceptable as the standby power source for each a-c load group of the size and characteristics typical of recent applications. If other arrangements such as multiple diesel generators operated in parallel or multiple prime movers driving a single generator are proposed, the applicant should demonstrate that the proposed arrangement has an equivalent reliability. Common mode failures as well as random single failures should be considered in the analysis.