Enhanced Power System Design for Nuclear Safety and Reliability

Mr. Thomas Koshy, Team Leader, Engineering Research Applications, Office of Nuclear Regulatory Research, United States Nuclear Regulatory Commission

Abstract

This paper describes certain design and operational approaches to enhance the power system design of nuclear power plants (NPPs) by eliminating or reducing the probability of many known problems identified through operating experience. Specifically, this paper addresses six known problems and describes solutions. (1) For inadequate voltage at the preferred power source when a nuclear station trips, this paper describes a contingency analysis program on the grid to provide adequate voltage by ensuring system capability following a loss of the largest generation source. (2) For electrical faults that propagate to more than one division at an NPP, enhanced design concepts with an additional breaker and a transformer could reduce common-mode failures between divisions. (3) For catastrophic failure of onsite breakers, strategic assignment of breaker position could limit damage and allow the remaining loads to operate until replacement breakers are ready for corrective maintenance. (4) For delays in safety bus energization, a design enhancement that avoids fast-transfer logic would allow immediate availability of offsite power from the grid. (5) For instrument bus power supply failures, this paper describes a mitigating strategy, in which the emergency diesel generator and bus protection system would be controlled with direct current (DC) power supported by backup battery power. (6) For plant trips and losses of offsite power caused by external faults at locations away from the plant, this paper describes increasing the sensitivity of the protection system at the NPP switchyard, and removing the auto-reclosing circuits.

Introduction

This paper describes certain design and operational approaches to enhance the power system design of nuclear power plants (NPPs) by eliminating or reducing the probability of six specific known problems identified through operating experience.

1. Inadequate Voltage at the Preferred Power Source When a Nuclear Station Trips

In many areas, NPPs are among the largest power generation sources on the local grid. As such, these plants generally carry the reactive loads and significantly contribute to voltage support. As a result, a trip of one of these NPPs produces significant stress on the local grid.

In such instances, inadequate NPP contingency post-trip switchyard voltages can lead to inoperability of the plant's offsite power system as a result of the actuation of the plant's degraded voltage protection circuits. These circumstances have also occasionally caused NPPs of certain designs to experience other inoperabilities, including overloaded emergency diesel generators (EDGs) or losses of certain safety features as a result of interaction with circuit breaker logic. In addition, these circumstances can cause safety-related motors to be started more than once in a short period, which could result in operation outside the motors' specifications, as well as actuation of overload protection. Moreover, the unavailability of plant-controlled electrical equipment, such as voltage regulators, transformer auto-tap changers, and automatic generator voltage regulators can contribute to the frequent occurrence of inadequate NPP post-trip voltages.

Analysis tools in use by transmission system operators (TSOs), together with properly implemented training and protocols for communication between the TSOs and NPP licensees, could help to ensure that plant operators are better informed about conditions affecting their offsite power systems. See Fig 1 for a communication road map. Toward that end, an online contingency analysis program to accurately predict the adequacy of the voltage at the preferred power source when a nuclear station trips is beneficial.

In the deregulated electric power environment, the power flow varies significantly based on market conditions. This variability of power flow makes it difficult to rely on offline analyses for the adequacy of offsite power. For that reason, contingency analyses for NPPs

should account for the impact of both normal and emergency shutdown loads on the transmission network (grid) immediately following a nuclear station trip.

The transmission network is the preferred source of power to the current generation of US NPP's accident mitigation system. Consequently, the United States Nuclear Regulatory Commission (NRC) established General Design Criterion (GDC) 17 in Appendix A to Title 10, Part 50, of the *United States Code of Federal Regulations* (10 CFR Part 50). Specifically, GDC 17 requires, in part, provisions to minimize the probability of losing electric power from any of the remaining supplies (including the transmission network) as a result of, or coincident with, the loss of power generated by the nuclear power unit (i.e., a trip). Because a trip is an anticipated operational occurrence, the offsite power circuits must be designed to be available following a trip to permit the functioning of safety system components. For that reason, the NRC further clarified its technical position in Regulatory Issue Summary (RIS) 2004-5, "Grid Reliability and the Impact on Plant Risk and the Operability of Offsite Power," and Generic Letter (GL) 2006-02, "Grid Reliability and the Impact on Plant Risk and the Operability of Offsite Power."

Consistent with the NRC's regulatory guidance, when a contingency analysis predicts an inadequate voltage condition for a nuclear station based on contingencies in the area, the NPP should refrain from risk-significant surveillances and implement suitable actions to provide an alternative source of power. Such actions reduce the probability of a station trip and prepare the NPP to deal with potential post-trip conditions.

2. Electrical Faults that Propagate to More Than One Division at an NPP

The common design practices to isolate electrical faults are generally effective; however, certain low-impedance faults can lead to catastrophic failures that destroy the circuit breaker and keep the upstream feeder cable in a faulted condition. Consequently, offsite power could be lost for both trains of safety buses. As shown in Figure 2, if the offsite power was connected to the safety buses through a single startup transformer, the feeder cable fault would prevent power supply to both safety buses. Enhanced design concepts with an additional breaker and a transformer could significantly reduce common-mode power supply failures between divisions.

3. Catastrophic Failure of Onsite Breakers

In 1995, the Waterford Generating Station experienced a catastrophic failure of a breaker that connects the offsite power to the plant bus (i.e., the offsite power feeder breaker). That event is described in detail in Licensee Event Report (LER) 05000382-95-002-01, which is available in the NRC's Agencywide Documents Access and Management System (ADAMS), under Accession No. ML9801160136). Briefly, in response to a lightning arrester failure, the protection scheme commanded a trip; however, the breaker failed with one of its phases remaining latched, and this led to a catastrophic failure. Fortunately, however, the offsite power feeder breaker was physically located at the extreme end of the bus. As a result, the plant was able to isolate the faulted breaker and continue plant operation using remaining part of the bus until breaker assemblies were procured and repairs were scheduled.

In general, the breakers that connect the offsite power to the plant bus are subjected to a greater number of cycles of operation, and interrupt the most fault current. Consequently, these offsite power feeder breakers have a higher probability of failure than other breakers. With this reality in mind, strategically assigning offsite power feeder breakers to the extreme ends of the bus could limit damage and allow the remaining loads to operate in case of a failure.

4. Delays in Safety Bus Energization

Most NPP safety buses are designed to receive power from the grid using "fast-transfer logic" in the event that the nuclear station trips. However, several failures in the power transfer scheme have occured. In particular, if the safety bus power feeds are taped from the grid after the main generator breaker (so that the grid can directly supply the station loads), the power from the grid will be available immediately following

the plant trip without the need for a power transfer. See the simplified Class 1E power system in Figure 3, which is essentially the same approach that the Institute of Electrical and Electronics Engineers (IEEE) conveys in Figure 4 of IEEE Std. 765–2006, "Standard for Preferred Power Supply (PPS) for Nuclear Power Generating Stations (NPGS)."

IEEE Std. 765–2006 further advocates directly feeding the safety bus, without any intervening non-safety-related buses. This approach offers the added benefit of limiting the transient torque when large motor-driven pumps are transferred to a different power source. Thus, the fast-transfer logic could be avoided through a design enhancement.

Another approach to solve this problem is to always align the offsite power to the safety buses to eliminate the need to transfer power to the bus. However, in certain market conditions, it is more economical to use an auxiliary transformer to feed the safety bus during power generation, rather than buying power from the grid.

In order to ensure continued availability of power from the grid to the safety buses, communication with the grid operator is very important, as described in GL 2006-02. When a nuclear station trips, a typical 1,000-MW power generation source becomes a 30-MW electrical load. The normal or emergency cool down can be accomplished from the grid power only if the grid voltage is above the under voltage setpoint. If the nuclear station and grid operation have different ownership, a contractual agreement is desirable to ensure adequate voltage and capacity for the station's safety buses. See Figure 1 for the suggested communication roadmap to ensure an adequate offsite power supply for NPPs.

In addition, as described in Section 1 (above), the grid operations must be managed with an online contingency analysis program. Moreover, that program must have the capability to respond to a trip of the largest generation unit or transmission system element, or the addition of an anticipated load. Such contingencies and disturbances must be resolved in no less than 15 minutes, to ensure that the system is ready to respond to the next probable contingency. The applicable procedures for the U.S. industry are available through the North American Electric Reliability Corporation (NERC) Web site, at http://www.nerc.com/~filez/standards/Reliability_Standards_Regulatory_Approved.html.

5. Instrument Bus Power Supply Failures

Vital bus failures primarily result from failure of the inverter and its switching mechanisms. The other components that influence vital power failures are battery chargers, EDGs, and the associated control systems.

There are two approaches to designing safety and non-safety instrument (vital) buses. One approach is to connect the protection system to an uninterruptible power supply (UPS) and design the logic to be failsafe (i.e., the failure mode of the system is to cause a reactor trip). The other approach is to design the Class 1E instrument bus (supporting the emergency core cooling systems) on a DC system, with a backup battery bus, battery charger, and EDG. If the vital bus must be an AC system, two or more inverters would be necessary to ensure continuity in the vital power supply. In either of these designs, it is desirable to provide DC power to sense under-voltage, EDG startup and operation, and controlling breakers for Class 1E loads (especially core cooling loads). (See Figure 4.)

In this way, instrument power supply failures could be mitigated by using DC power, supported with backup battery power, to control the EDG and the bus protection system.

6. Plant Trips and Losses of Offsite Power Caused by External Faults

NRC Information Notice (IN) 2005-15, "Three-Unit Trip and Loss of Offsite Power at Palo Verde Nuclear Generating Station," and IN 2007-14, "Loss of Offsite Power and Dual-Unit Trip at Catawba Nuclear Generating Station," discuss two events in which an electrical fault at a significant distance from an NPP caused a multiunit trip and loss of all offsite power. In each case, one of the units at a multiunit plant encountered a problem with one of its EDGs.

These examples illustrate that external faults located at a significant distance from the plant have been responsible for causing several plant trips and/or losses of offsite power. Such instances pose challenges to control room operations. The substation serving the NPP has a significant influence in plant trips and the availability of offsite power. While a plant trip may accrue a significant loss of revenue, the loss of offsite power has far more significant safety implications for plants that rely on offsite power as the preferred source of power for accident mitigation.

One approach to solve this issue is to modify the bases for the substation's electrical protection system to achieve greater protection than the power availability. In order to localize electrical faults, a selective tripping technique is used, which involves providing sufficient time delays for the first level of protection to clear the fault. The traditional time permitted for first-level protection could be reduced to induce a preemptive trip to protect the NPP substation. Although this approach would reduce availability for certain circuits, it would yield a benefit by preventing a nuclear unit trip resulting from either loss of load or actuation of backup protection to clear an electrical fault.

Along with differential current protection and stuck breaker protection, ground fault detection could be installed in each segment of the substation to instantaneously clear any significant ground fault. Auto-reclosing circuits, which are generally prevalent in the transmission system, could be executed differently. Specifically, following a trip of the feeder, these circuits could be energized from a source other than the nuclear substation. TSO could then verify that the fault has cleared before connecting the circuit to the nuclear substation. These steps can significantly reduce challenges to offsite power and trips of nuclear stations.

Conclusion

The reliability of offsite power support could be significantly improved through design modifications and operational controls. Some of the suggested approaches are convenient only for new NPP designs. Nonetheless, certain benefits to be realized may outweigh the cost of design modifications — especially for plants that have offsite power as the preferred source of power for accident mitigation. Moreover, because the power supply requirements for an NPP are not typical of the industry requirements, a greater level of coordination between the TSOs and NPP licensees would ensure continued voltage and capacity support for accident mitigation.

References

1. *United States Code of Federal Regulations* Title 10, Part 50, of the (10 CFR Part 50) General Design Criterion (GDC) 17 in Appendix A
2. Regulatory Issue Summary (RIS) 2004-5, "Grid Reliability and the Impact on Plant Risk and the Operability of Offsite Power
3. Generic Letter (GL) 2006-02, "Grid Reliability and the Impact on Plant Risk and the Operability of Offsite Power
4. Licensee Event Report (LER) 05000382-95-002-01
5. IEEE Std. 765–2006, "Standard for Preferred Power Supply (PPS) for Nuclear Power Generating Stations
6. http://www.nerc.com/~filez/standards/Reliability_Standards_Regulatory_Approved.html
7. NRC Information Notice (IN) 2005-15, "Three-Unit Trip and Loss of Offsite Power at Palo Verde Nuclear Generating Station
8. IN 2007-14, "Loss of Offsite Power and Dual-Unit Trip at Catawba Nuclear Generating Station

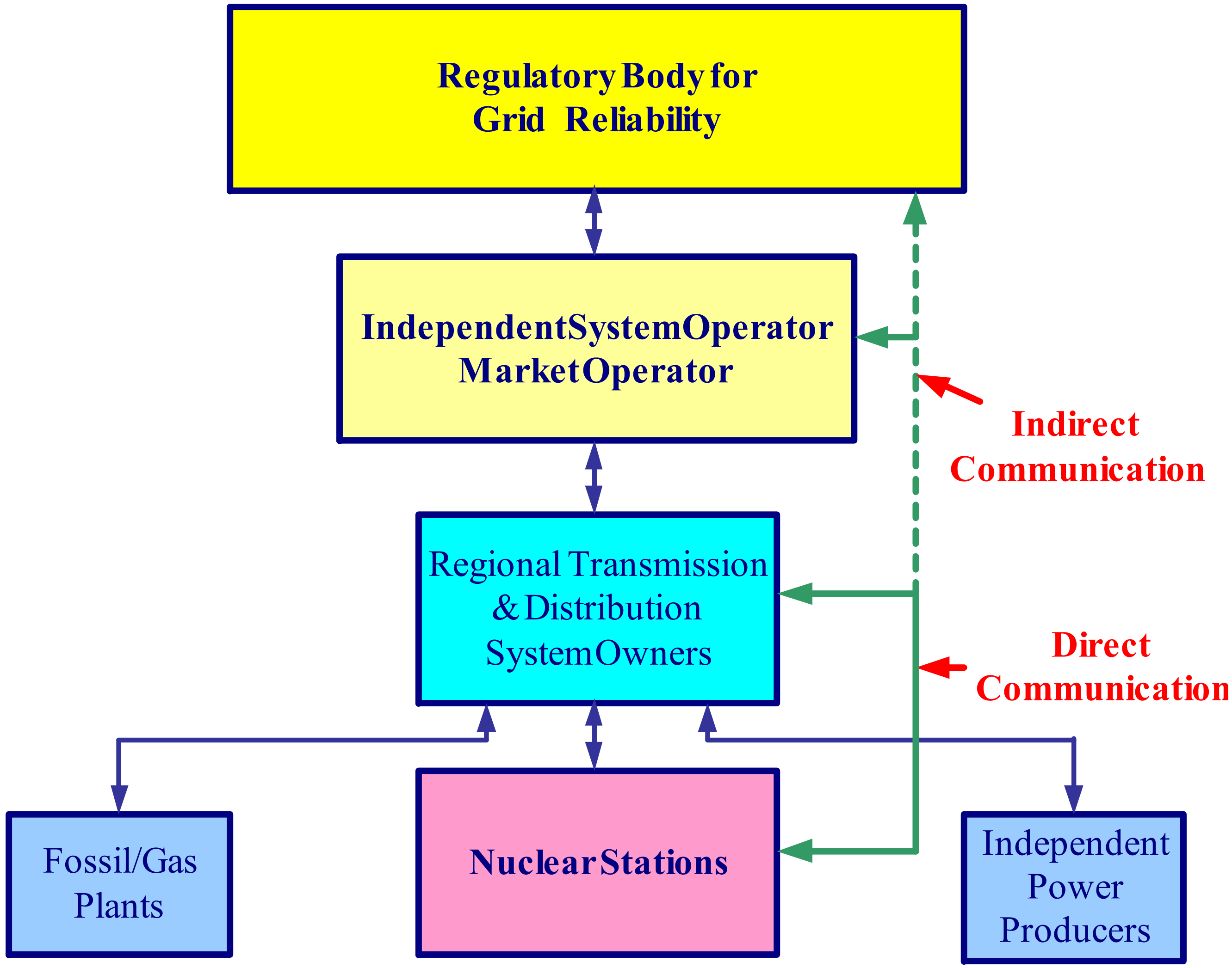
Regulatory Body for Grid Reliability
Independent System Operator Market Operator
Regional Transmission & Distribution System Owners
Fossil/Gas Plants
Nuclear Stations
Independent Power Producers
Indirect Communication
Direct Communication

Fig 1

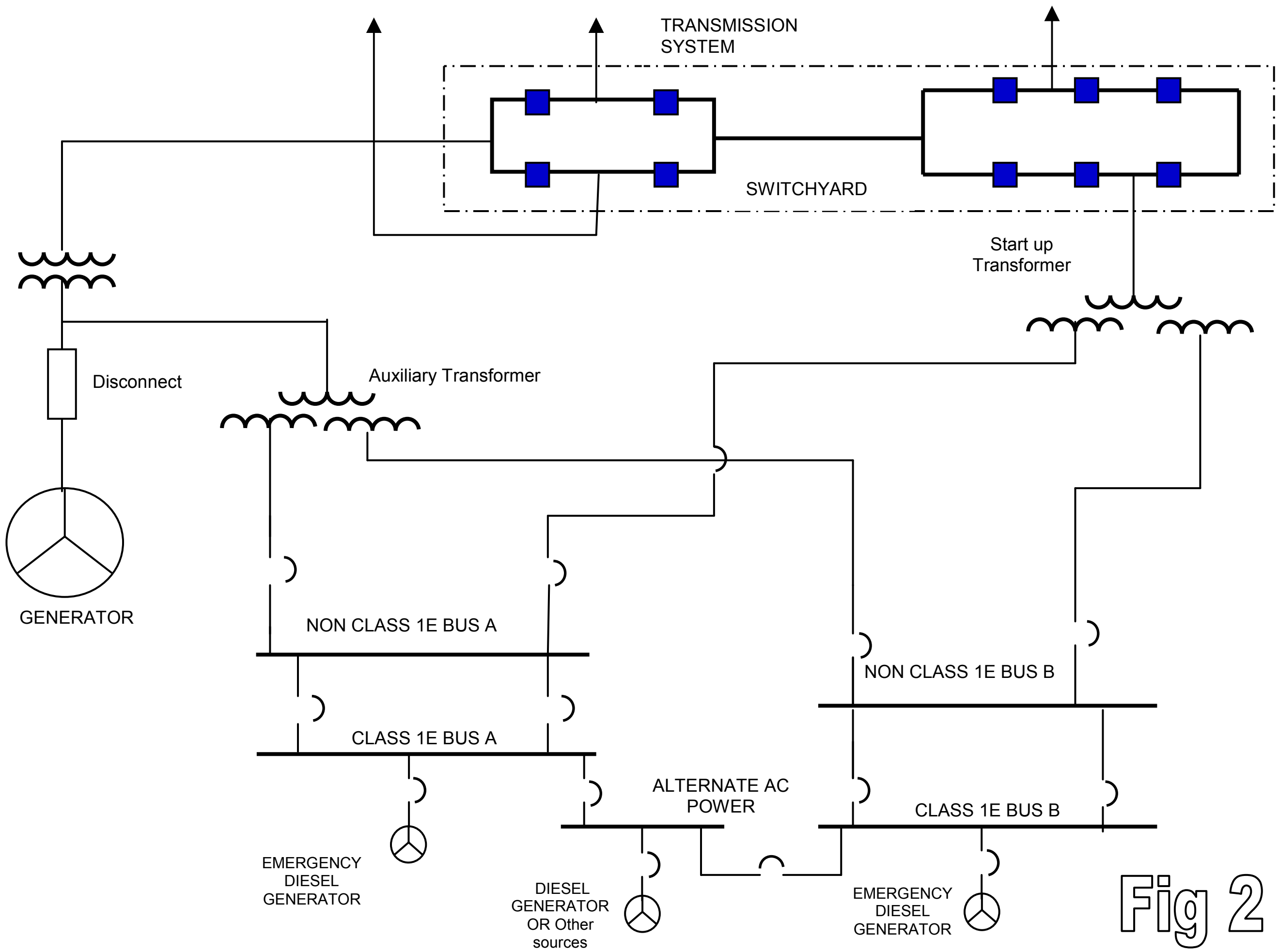
TRANSMISSION SYSTEM
SWITCHYARD
Start up Transformer
Disconnect
Auxiliary Transformer
GENERATOR
NON CLASS 1E BUS A
CLASS 1E BUS A
NON CLASS 1E BUS B
CLASS 1E BUS B
ALTERNATE AC POWER
EMERGENCY DIESEL GENERATOR
DIESEL GENERATOR OR Other sources
EMERGENCY DIESEL GENERATOR

Fig 2

ONE LINE DIAGRAM FOR SINGLE UNIT NUCLEAR STATION

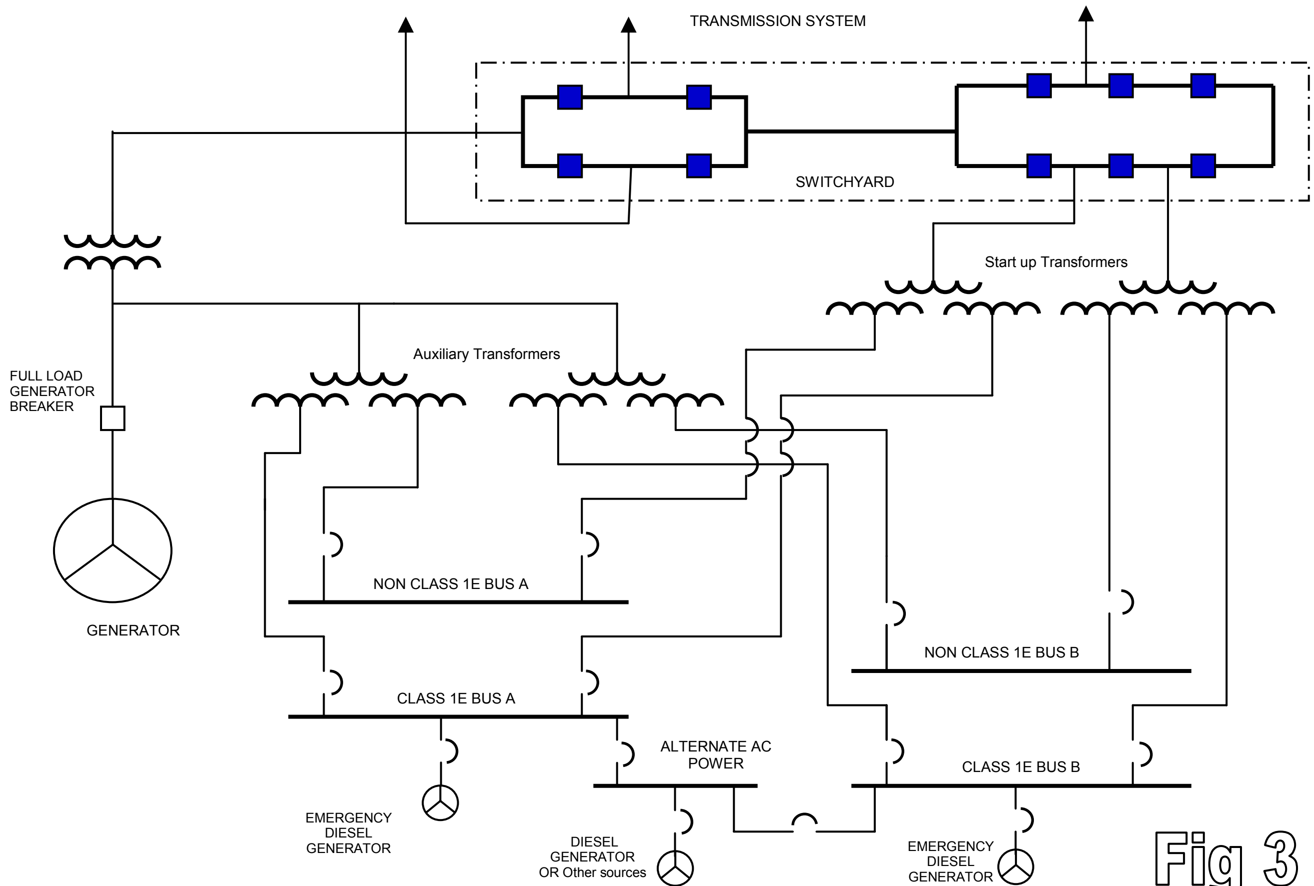

Fig 3

Simplified Class 1E Power System

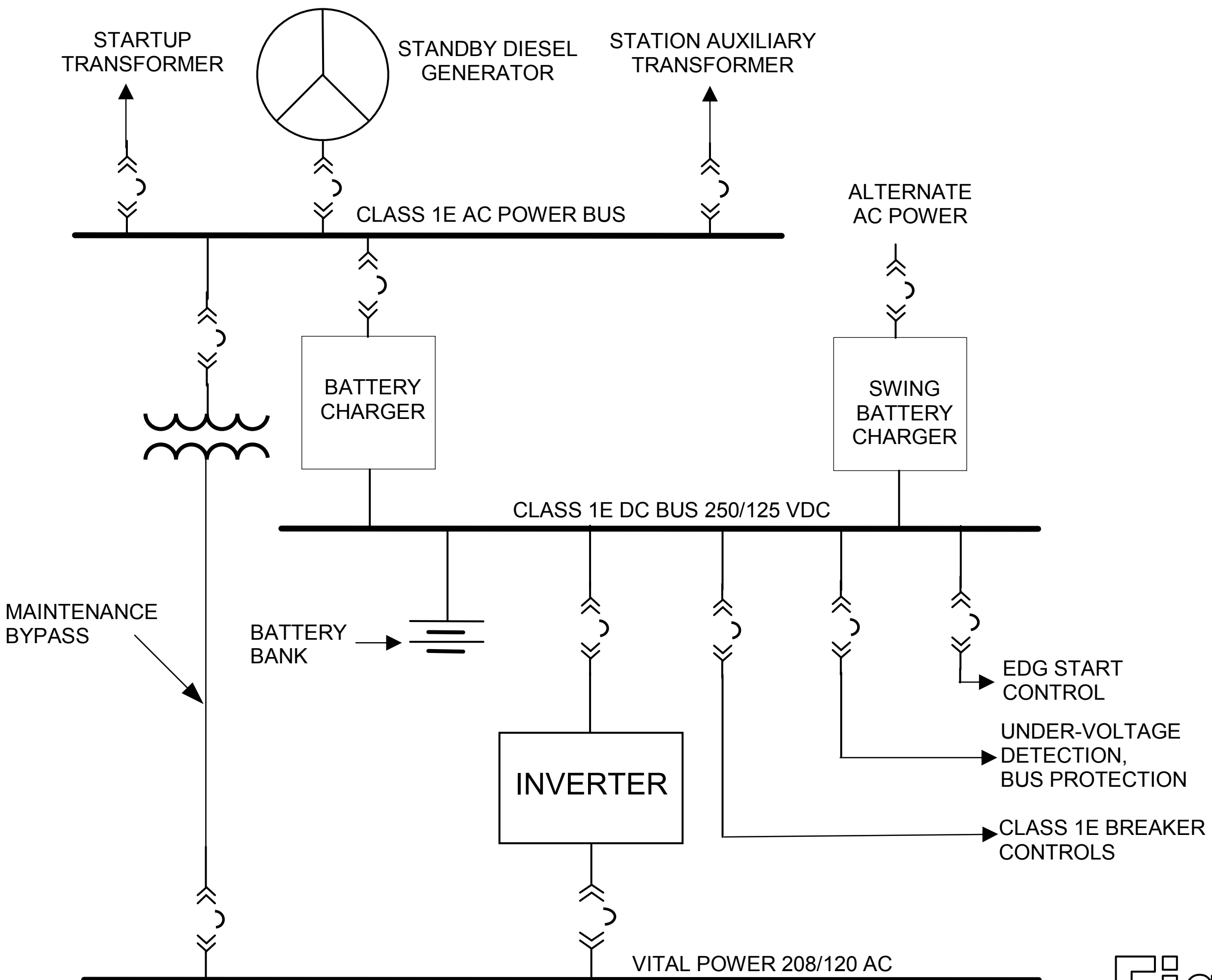

Fig 4