8. ELECTRIC POWER SYSTEMS

8.1 Introduction

The AP1000 design as presented does not require Class 1E alternating current (ac) electrical power, except that provided by the Class 1E direct current (dc) batteries and their inverters, to accomplish the plant's safety-related functions.

As the bases for evaluating the adequacy of the design of the Class 1E dc batteries and their inverters, to accomplish the plant's safety-related functions as presented in AP1000 Design Control Document (DCD) Tier 2, Chapter 8, "Electric Power," the U.S. Nuclear Regulatory Commission (the NRC or staff) used the acceptance criteria and guidelines for electric power systems contained in Chapter 8, "Electric Power," of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants—LWR Edition" (SRP); Regulatory Guide (RG) 1.153, "Criteria for Safety Systems"; RG 1.155, "Station Blackout"; and Section 50.63 of Title 10 of the Code of Federal Regulations (CFR), "Loss of All Alternating Current Power." Although these guidelines pertain to Class 1E equipment, the staff considered them in its review of the overall adequacy of the Westinghouse AP1000 simplified passive advanced light-water reactor (ALWR) electric power systems.

In SECY-95-132, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems (RTNSS) in Passive Plant Designs," the NRC set forth policy regarding those systems in passive light-water reactors that are designated non-safety-related, but that may have a significant role in accident and consequence mitigation. Section 8.5.2.3 of this report discusses the specific aspects of electric power systems that are designated as RTNSS.

8.2 Offsite Power System

Regulatory Evaluation

The offsite power system includes two or more physically independent circuits capable of operating independently of the onsite standby power sources. The staff's review covers the information, analyses, and documents for the offsite power system and the stability studies for the electrical transmission grid. The review focuses on the basic requirement that the loss of the nuclear unit, which is the largest operating unit on the grid, or the loss of the most critical transmission line will not result in the loss of offsite power to the plant. SRP Branch Technical Position (BTP) Instrumentation and Control Systems Branch (ICSB)-11, "Stability of Offsite Power Systems," and General Design Criteria (GDC) 17, "Electric Power Systems," of 10 CFR Part 50 outline an acceptable approach to addressing the issue of stability of offsite power systems. Specific review criteria are contained in SRP Section 8.1, "Electric Power," SRP Section 8.2, "Offsite Power System," Appendix A to SRP Section 8.2, BTP Power Systems Branch (PSB)-1, "Adequacy of Station Electric Distribution System Voltages," and ICSB-11.

Technical Evaluation

The staff consulted the guidance documents specified in Section 8.1 of this report. Additional considerations pertain to the non-Class 1E portion of the electrical design with respect to RTNSS. See Section 8.5.2.3 of this report for a discussion regarding RTNSS.

The applicant shares the AP1000 design responsibility for the offsite power system with the combined license (COL) applicant referencing the design. The requirements imposed on the COL applicant's design by the AP1000 design are specified by interface requirements or COL action items. See Section 8.2.3 of this report for a discussion of COL action items.

8.2.1 Offsite Circuits Outside the AP1000 Scope of Design

The utility company grid system and its interconnection to other grid systems and generating stations are site specific. Section 8.2.3 of this report discusses specific COL action items with respect to this subject area.

8.2.2 Offsite Circuits within the AP1000 Scope of Design

The AP1000 electrical system design scope encompasses the plant from the high side of the main power transformer, and from the high side of the reserve auxiliary transformer (provided for maintenance).

The main generator normally provides power to the main ac power system. When the main generator is not available, the generator output breaker is opened and the plant auxiliary power comes from the switchyard by backfeeding through the main step-up transformers and the unit auxiliary transformers (UAT). In addition, two non-Class 1E onsite standby diesel generators supply power to selected loads in the event of loss of either the main generator or the main transformer. There is also a maintenance source provided through a reserve auxiliary transformer (RAT). The maintenance source is site specific, and bus transfer to the maintenance source is manual. Maintenance power is provided at the medium voltage level of 6.9 kilovolts (kV).

The main generator is connected to the offsite power system by three single-phase, main step-up transformers. The generator buses provide the normal power source for the plant auxiliary ac loads through two unit auxiliary transformers of identical rating. In the event of a loss of the main generator, an auto-trip of the main generator breaker maintains the power without interruption from the preferred power supply. The power then flows from the switchyard to the auxiliary loads through the main and unit auxiliary transformers. A spare single-phase, main transformer is provided, and it can be placed in service upon failure of one phase of the main step-up transformers.

The staff considers that the information provided is sufficient and is therefore acceptable.

8.2.3 Offsite Power System Interfaces

The operating voltage for the high side of the AP1000 transformer and transmission switchyard, as well as the frequency decay rate, are site specific and, therefore, will be addressed in the COL application. The staff will provide further review of the operating voltage and the frequency decay rate when a COL applicant submits its application. This COL information is discussed in DCD Tier 2, Section 8.2.5, "Combined License Information for Offsite Electrical

Power," and in Item 8.3 of DCD Tier 2, Table 1.8-1, "Summary of AP1000 Plant Interfaces with Remainder of Plant." Therefore, the operating voltage and the frequency decay rate is COL Action Item 8.2.3-1.

8.2.3.1 Grid Stability

The AP1000 is designed with passive safety-related systems for core cooling and containment integrity and, therefore, does not depend on the electric power grid for safe operation. This feature of the AP1000 design significantly reduces the importance of grid connection and grid stability. The AP1000 safety analyses assume that the reactor coolant pumps (RCPs) can receive power at 6.9 kV from either the main generator or the grid for a minimum of 3 seconds following a turbine trip. The AP1000 design has a generator circuit breaker on the output of the main generator and utilizes backfeed from the grid to maintain power to the RCPs following a turbine/generator trip.

If during power operation of the plant, a turbine trip occurs, the motive power to the turbine will be removed. The generator will keep the shaft rotating at synchronous speed (governed by the grid frequency) by acting like a synchronous motor. The reverse power relay, which monitors generator power, will sense this condition and, after a time delay of at least 15 seconds, open the generator breaker. During this time delay, the generator will provide voltage support to the grid, if needed. The RCPs will receive power from the grid for at least 3 seconds following a turbine trip.

The COL applicant will perform a grid stability analysis to show that the grid will stay stable and that the RCP bus voltage will remain above the voltage required to maintain the flow assumed in DCD Tier 2, Chapter 15, "Accident Analyses," for a minimum of 3 seconds following a turbine trip. This COL information is discussed in DCD Tier 2, Section 8.2.5, "Combined License Information for Offsite Electrical Power," and in Item 8.3 of DCD Tier 2, Table 1.8-1, "Summary of AP1000 Plant Interfaces with Remainder of Plant." This is COL Action Item 8.2.3.1-1.

The COL applicant will set the protective devices controlling the switchyard breakers in such a way as to preserve the grid connection following a turbine trip. This COL information is discussed in DCD Tier 2, Section 8.2.5, "Combined License Information for Offsite Electrical Power," and in Item 8.3 of DCD Tier 2, Table 1.8-1, "Summary of AP1000 Plant Interfaces with Remainder of Plant." This is COL Action Item 8.2.3.1-2.

If the turbine trip occurs when the grid is not connected (generator supplying house loads only), the main turbine generator shaft will begin to slow down as the energy stored in the rotational inertia of the shaft is used to supply the house loads (including the RCPs). The system will coast down until the generator exciter can no longer maintain generator terminal voltage and the generator breaker is tripped based on either generator undervoltage or exciter overcurrent. The coastdown will last at least 3 seconds before the generator breaker trips.

The sequence of events following a loss of offsite power is the same as that described for grid disconnected operation. The sequence of events provides additional assurance that the main generator will be available to support grid voltage, if needed, for the 3 seconds assumed in the DCD Tier 2, Chapter 15 analysis.

Because of certain electrical failures (such as a loss of isophase bus), power from the generator or grid may not be available to the RCPs for a minimum of 3 seconds following a turbine trip. The COL applicant must perform a failure modes and effects analysis (FMEA) to ensure that the design provides power to the RCPs for a minimum of 3 seconds following a turbine trip. If the power to the RCPs cannot be maintained for 3 seconds, then the DCD Tier 2, Chapter 15 analysis should be reanalyzed and provided to the staff for review. Open Item 8.2.3.1-1 in the Draft Safety Evaluation Report (DSER) identified the need for inclusion of this COL information in the DCD.

The applicant provided a response to DSER Open Item 8.2.3.1-1 by letter dated July 31, 2003. The response stated that the isophase bus is a passive component that must be operational for the turbine generator to be operated. Because the isophase bus is required for power operation, it is known to be operational at the start of the 3-second time period. The failure of a passive component that is known to be initially operational within a 3-second window is a very low probability event. The applicant revised DCD Tier 2, Section 8.2.2 to state the following:

> The Combined License applicant will perform a grid stability analysis to show that, with no electrical system failures, the grid will remain stable and the reactor coolant pump bus voltage will remain above the voltage required to maintain the flow assumed in the Chapter 15 analyses for a minimum of 3 seconds following a turbine trip. In the Chapter 15 analyses, if the initiating event is an electrical system failure (such as failure of the Isophase bus), the analyses do not assume operation of the reactor coolant pumps following the turbine trip.

This is COL Action Item 8.2.3.1-3.

The staff concludes that the electrical features described in the AP1000 DCD can provide power, assuming no electrical system failures, either from the main generator or from the grid, to the RCPs following a turbine trip for a minimum of 3 seconds. However, for those initiating events involving electrical system failures, the analyses do not assume operation of the RCPs following a turbine trip and therefore the availability of power to the RCPs is not a concern. The staff has evaluated the applicant's response and the modifications in the DCD and concludes that the applicant has adequately addressed Open Item 8.2.3.1-1 and, therefore, the open item is resolved.

8.2.3.2 Conformance to Criteria (Part Exemption from GDC 17 for AC Offsite Power Sources)

The AP1000 design does not require ac power sources to mitigate design-basis events. Although the AP1000 is designed with reliable non-safety-related offsite and onsite ac power sources that are normally expected to be available for important plant functions, non-safety-related ac power is not relied upon to maintain core cooling or containment integrity. DCD Tier 2, Section 3.1, "Conformance with Nuclear Regulatory Commission General Design Criteria," states that the AP1000 design supports an exemption to the requirements of GDC 17, for two physically independent offsite circuits, by providing safety-related passive safety systems for core cooling and containment integrity.

A reliable dc power source supplied by batteries provides power for the safety-related valves and instrumentation during transient and accident conditions. The Class 1E dc and uninterruptible power supply (UPS) system is the only safety-related power source required to monitor and actuate the safety-related passive systems. Otherwise, the plant is designed to maintain core cooling and containment integrity, independent of non-safety-related ac power sources indefinitely. The non-safety ac power system is designed such that plant auxiliaries can be powered from the grid under all modes of operation. During loss of offsite power (LOOP), ac power is supplied by the onsite standby diesel generators. The onsite standby power system is not required for safe shutdown of the plant.

Pursuant to 10 CFR 52.48, "Standards for review of applications," applications filed under this subpart will be reviewed for compliance with the standards set out in 10 CFR Part 20, Part 50 and its appendices, and Parts 73 and 100 as they apply to applications for construction permits and operating licenses for nuclear power plants, and as those standards are technically relevant to the design proposed for the facility. The requirements of GDC 17 are set forth in Appendix A to Part 50.

Pursuant to 10 CFR 50.12, "Specific Exemption," the Commission may, upon application by any interested person or upon its own initiative, grant exemptions from the requirements of 10 CFR Part 50 when (1) the exemptions are authorized by law, will not present an undue risk to public health or safety, and are consistent with the common defense and security; and (2) when special circumstances are present. Special circumstances are present whenever, according to 10 CFR 50.12(a)(2)(ii), "Application of the regulation in the particular circumstances would not serve the underlying purpose of the rule or is not necessary to achieve the underlying purpose of the rule."

The underlying purpose of the requirement of GDC 17 to provide two offsite power sources to the plant is to ensure sufficient power to accomplish safety functions. The AP1000 design does not rely on power from the offsite system to accomplish safety functions, and therefore, the underlying purpose of the rule is met without the need for two independent offsite circuits. The staff concludes that special circumstances exist, in that, the regulation need not be applied in this particular circumstance to achieve the underlying purpose of having two offsite power sources. This meets the requirements for an exemption to GDC 17, as described in 10 CFR 50.12. Therefore, the staff concludes that an exemption to the requirements of GDC 17 for two physically independent offsite circuits is justified.

8.2.3.3 Testing and Inspection of the Offsite Power System

GDC 18, "Inspection and Testing of Electric Power Systems," requires that electric power systems important to safety shall be designed with the following capabilities:

- the ability to permit appropriate periodic inspection and testing of important areas and features (such as wiring, insulation, connections, and switchboards) to assess the continuity of the systems and the condition of their components

- the ability to periodically test the operability and functional performance of the components of the systems

- the ability to periodically test the operability of the systems as a whole (under conditions as close to design as practical) and the full operation sequence that brings the systems into operation

DCD Tier 2, Section 8.2.5 states that the COL applicants referencing the AP1000 certified design will address the design of the ac power transmission system and its testing and inspection plan. The testing and inspection capability of the system will provide conformance with GDC 18. This is COL Action Item 8.2.3.3-1.

8.2.3.4 Specific Interface Requirements for Supporting Chapter 15 Analyses

In the case of events involving a turbine trip, the applicant assumes that a LOOP, and the resulting coastdown of the RCPs, occurs 3 seconds after the turbine trip. The basis for the 3-second delay is provided in DCD Tier 2, Section 8.2, "Offsite Power System." This section describes the electrical design features of the AP1000, the electrical system response to a turbine trip, and the COL applicant interfaces that support the 3-second assumption. The AP1000 design provisions include the following electrical features that support the 3-second delay:

- An output generator circuit breaker and reverse power relay, with at least a 15-second delay before tripping the breaker following a turbine trip, will be used. This allows the generator to provide voltage support to the grid and maintain adequate voltage to the RCPs for significantly longer than the assumed 3 seconds.

- COL applicant interface Item 8.3 in DCD Tier 2, Table 1.8-1 states that transient stability must be maintained and the RCP bus voltage must stay above the voltage required to maintain the flow assumed in DCD Tier 2, Chapter 15 analyses for a minimum of 3 seconds following a turbine trip. This ensures that, for Westinghouse's unique grid system configuration, a grid instability condition following a turbine trip will take at least 3 seconds to result in a loss of power to the RCPs.

- COL applicant interface Item 8.3 in DCD Tier 2, Table 1.8-1 states that the protective devices controlling the switchyard breakers are set with consideration for preserving the plant grid connection following a turbine trip. This is especially important in generator output circuit breaker designs to ensure that the backfeed offsite circuit, through the generator main stepup transformer, is not interrupted by opening of the switchyard breakers following a turbine trip.

- No automatic transfers of RCP buses are used in the design (this precludes bus transfer failures following a turbine trip).

- If a turbine trip occurs when the grid is not connected to the plant, the main generator will be available to power the RCPs for at least 3 seconds before the generator output breaker is tripped based on either generator undervoltage or exciter overcurrent.

The staff concludes that the electrical features described in the AP1000 DCD can provide power to the RCPs following a turbine trip for a minimum of 3 seconds, either from the main generator or from the grid.

8.2.3.5 Conclusions

With respect to the offsite power system interfaces, the staff considers the applicant's description to be acceptable on the basis that sufficient information is provided for the scope of the offsite circuit. Further, pursuant to 10 CFR 50.12, the staff considers acceptable an exemption to the requirements of GDC 17 concerning the need for two offsite power sources. Therefore, the staff concludes that the design of the offsite power system for the AP1000 is acceptable.

8.3 Onsite Power Systems

8.3.1 AC Onsite Power System

Regulatory Evaluation

The onsite ac power system is a non-Class 1E system that provides reliable ac power to the various system electrical loads. It does not perform any safety-related functions. These loads enhance an orderly shutdown under emergency (not accident) conditions. Additional loads for investment protection can be manually loaded on the standby power supplied. The staff's review covers the descriptive information, analyses, and referenced documents for the ac onsite power system, as well as the applicable recommendations from NUREG/CR-0660, "Enhancement of On-site Emergency Diesel Generator Reliability."

Technical Evaluation

The main onsite ac power system is a non-Class 1E system which does not perform any safety-related function. During power generation mode, the turbine generator normally supplies electric power to the plant auxiliary loads through UATs. The plant is designed to sustain a load rejection from 100 percent power, with the turbine generator supplying the plant house loads.

During plant startup, shutdown, and maintenance, the generator breaker is opened. Under this condition, the main ac power is provided by the preferred power supply system from the high voltage switchyard (switchyard voltage is site specific) through the main step-up transformers and two UATs. Each UAT supplies power to about 50 percent of the plant loads. The UATs have two identically rated 6.9 kV secondary windings.

The maintenance source and the associated RAT primary voltage, are site specific. The RAT is sized to replace any one of the UATs, if needed. The availability of the RAT, provides operational flexibility if any of the UATs are out of service.

The buses tagged with odd numbers (ES1, ES3, etc.) are connected to one UAT, while the buses tagged with even numbers (ES2, ES4, etc.) are connected to the other UAT. These 6.9 kV buses are provided with access to the maintenance source through normally open circuit breakers connecting the bus to the RAT. Bus transfer to the maintenance source is manual.

The arrangement of the 6.9 kV buses permits feeding functionally redundant pumps or groups of loads from separate buses, and enhances the plant's operational flexibility. The RCPs are powered from the four 6.9 kV switchgear buses (ES3, ES4, ES5, and ES6) located in the turbine building. Each bus powers one RCP. Variable speed drives are provided for RCP startup and operation when the RCP temperature is less than 232.2 °C (450 °F). During normal power operation, with RCP temperatures above 232.2 °C (450 °F), 60 Hertz (Hz) power is provided directly to the RCPs, and the variable-speed drives are not connected. Each RCP is powered through two Class 1E circuit breakers connected in series. These are the only Class 1E circuit breakers used in the main ac power system for the specific purpose of satisfying the safety-related tripping requirement of these pumps. These Class 1E breakers assure that the RCPs trip during accident scenarios. The control power for each RCP trip circuit is provided by its respective Class 1E 125 Vdc system.

The staff considers that the information provided is sufficient and is therefore acceptable.

8.3.1.1 Electric Circuit Protection

The major types of protection systems employed for AP1000 include the following:

Medium Voltage Switchgear

Each medium voltage switchgear bus is provided with a bus differential relay (device 87B) to protect against a bus fault. The actuation of this relay initiates tripping of the source incoming circuit breaker and all branch circuit load breakers. The differential protection scheme employs high speed relays. Motors rated 1500 kilovoltampere (kVA) (1500 horsepower [hp]) and above are generally provided with a high dropout overcurrent relay (device 50D) for differential protection.

To provide the backup protection for the buses, the source incoming circuit breakers are equipped with an inverse time overcurrent relay on each phase and an inverse time ground fault relay for bus protection. Each medium voltage motor feeder breaker is equipped with a motor protection relay, which provides protection against various types of faults (phase and ground) and abnormal conditions such as locked rotor and phase unbalance. Each medium voltage power feeder to a 480 volt (V) load center has short circuit, overload, and an overcurrent protection for ground fault.

Medium voltage buses are provided with a set of three undervoltage relays (27B) that trip feeder circuit breakers connected to the bus upon a complete loss of ac power, using two-out-of-three logic, to prevent spurious actuation. In addition, another set of undervoltage relays is provided on the line side of the incoming supply breakers of buses ES1 and ES2. These relays initiate an alarm in the main control room (MCR) if a sustained low- or high-voltage condition occurs.

Medium voltage switchgears (ES1 and ES2) are located in the electrical switchgear rooms 1 and 2 of the annex building. Switchgears ES3, ES4, ES5, and ES6 are located in the turbine building electrical room. The Class 1E medium voltage switchgear for four RCPs is located in the turbine building. The control power for each RCP trip circuit is provided by its respective Class 1E 125 Vdc system.

480 V Load Centers

Each motor feeder breaker in load centers is equipped with a trip unit, which has long-time, instantaneous, and ground fault tripping features. Each load center bus has an undervoltage relay that initiates an alarm in the MCR upon loss of bus voltage.

480 V Motor Control Center

Motor control center (MCC) feeders for low voltage (460 V) motors have molded case circuit breakers (magnetic or motor circuit protectors) and motor starters. These motor starters are provided with thermal overload protection. Non-Class 1E ac motor-operated valves are protected by thermal overload devices.

The applicant has addressed the major types of electric circuit protection systems and has provided sufficient information.

8.3.1.2 Standby Diesel Generators

The onsite standby power system, powered by the two onsite standby diesel generators, provide 4000 kilowatts (kW) each to selected loads in the event of a loss of normal and preferred ac power supplies. The system's function is to provide a backup source of electrical power to onsite equipment needed to support the decay heat removal operation during reduced reactor coolant system inventory and midloop operation. Those loads, which are priority loads for the defense-in-depth function based on their specific functions (permanent, non-safety loads), are assigned to annex building buses ES1 and ES2. These permanent, non-safety loads are divided into two functionally redundant load groups.

Separate sources provide power supplies to each diesel generator subsystem component to maintain reliability and operability of the onsite standby power system. The source incoming breakers on switchgear ES1 and ES2 are interlocked to prevent inadvertent connection of the onsite standby diesel generator and preferred/maintenance ac power sources to the 6.9 kV buses at the same time. The diesel generator, however, is capable of being manually paralleled with the preferred power supply for periodic testing. Design provisions protect the diesel generators from excessive loading, beyond the design maximum rating, should the preferred power be lost during periodic testing. The control scheme, while protecting the diesel generators from excessive loading, does not compromise the onsite power supply's ability to support the defense-in-depth loads. The standby diesel generators are included in the investment protection short-term availability controls.

If a loss of the preferred power source occurs concurrently with the turbine-generator trip, the diesel generators are automatically started and connected to the associated medium voltage buses, should these buses experience a loss of voltage. The following conditions are prerequisites for the diesel generator automatic start:

- starting air pressure within acceptable limits
- dc control power availability for fuel oil valve solenoid operation and the starting air motor solenoid
- fuel supply availability
- diesel generator controls in the automatic mode
- diesel generator breaker lockout trip permissive not activated by any of the trouble conditions
- engine prelubrication provided

Satisfactory status of these "prestart" conditions continuously monitored, and any failure will be annunciated in the MCR.

The starting air subsystem consists of an ac motor-driven, air-cooled compressor and an air receiver with sufficient stored capacity for three diesel engine starts. The diesel generator engine fuel oil system consists of an engine-mounted, engine-driven fuel oil pump that takes fuel from the fuel oil day tank. The lubrication system is contained on the engine skid and includes an engine oil sump, a main engine driven oil pump, and a continuous engine prelube system consisting of an ac and dc motor-driven prelube pump and electric heater. The prelube system maintains the engine lubrication system in service when the diesel engine is in standby mode.

Each diesel generator is a direct-shaft-driven, air-cooled self-ventilated machine. The generator component design is in compliance with the National Electrical Manufacturers Association (NEMA) Standard MG-1, "Motors and Generators." Each generator produces its rated power at 6900 V, 60 Hz. Each generator's continuous rating is based on supplying the non-safety electrical loads which provide shutdown capability using non-safety-related systems. The generators can also provide power for additional investment protection ac loads manually after the loads required for orderly shutdown have been satisfied. The selected unit rating has a design margin to accommodate possible derating resulting from other site conditions. The diesel generator unit is able to reach the rated speed and voltage, and can be ready to accept loads, within 120 seconds after a start signal. The generator exciter and voltage regulator systems are capable of providing full voltage control during operating conditions including postulated fault conditions. Each generator has an automatic load sequencer to enable controlled loading on the generator. The automatic load sequencer connects selected loads at predetermined intervals. This feature allows recuperation of generator voltage and frequency to rated values prior to the connection of the next load.

To enable periodic diesel generator testing, each generator is synchronized to a local panel, as well as to the MCR. Each standby diesel generator is tested to verify its capability to provide 4000 kW while maintaining the output voltage and frequency within the design tolerances of 6900±10 percent Vac and 60±5 percent Hz. The test duration will be the time required to reach engine temperature equilibrium plus 2.5 hours. This duration is sufficient to demonstrate long-term capability.

Preoperational tests are conducted to verify proper operation of the ac power system. The preoperational tests include operational testing of the diesel load sequencer and diesel generator capacity testing. The diesel generators are not safety-related and will be maintained in accordance with the requirements of the overall plant maintenance program. This program will cover the preventive, corrective, and predictive maintenance activities of the plant systems and equipment and will be presented in the COL application. This COL information is discussed in DCD Tier 2, Section 8.3.3, “Combined License Information for Onsite Electrical Power.” This is COL Action Item 8.3.1.2-1.

The applicant has provided sufficient information to demonstrate that the standby diesel generator is capable of providing a backup source of electrical power to onsite equipment needed to support decay heat removal operation during reduced reactor coolant system inventory and midloop operation.

8.3.1.3 Ancillary ac Diesel Generators

The applicant has included two ancillary diesel generators located in the annex building to provide power to meet the post-72 hour power requirements following an extended loss of offsite power sources. Each ancillary diesel generator output is connected to a distribution panel. The outgoing feeder circuits from the distribution panel are connected to cables which are routed to the Divisions B and C voltage regulating transformers and to the passive containment cooling system (PCS) pumps. Class 1E voltage regulating transformers power the post-accident monitoring loads, the lighting in the MCR, and ventilation in the MCR and Divisions B and C instrumentation and control (I&C) rooms. It also provides power to support operation of the ancillary generator’s lighting and fuel tank heating equipment. The ancillary diesel generators are not needed for refilling the PCS water storage tank, post-accident monitoring, or lighting for the first 72 hours following a loss of all other ac sources. They also are not needed for spent fuel makeup for the first 7 days following the loss of all other ac sources.

The generators are commercial-grade, skid-mounted packaged units, and are seismically designed. Generator control is manual from a control integral with the diesel skid package. The fuel for ancillary generators is stored in a tank located in the same room as the generators. This tank is analyzed to show that it will withstand a safe-shutdown earthquake (SSE) and holds sufficient fuel for 4 days of operation. Each ancillary diesel generator is tested to verify the capability to provide 35 kW, while maintaining the output voltage and frequency within the design tolerances of 480±10 percent Vac and 60±5 percent Hz. The 35 kW capacity is sufficient to meet the post-72 hours nominal load requirement.

Based on the ancillary ac diesel generator capabilities described above, the staff concludes that the ancillary ac diesel generators are acceptable as backup power sources for the longer term (post-72 hours) following a loss of all other ac power sources. Therefore, the staff finds the ancillary ac diesel generators to be acceptable.

8.3.1.4 Heat Tracing System

The electric heat tracing system is non-safety-related and provides electrical heating where a temperature above ambient is required for system operation and freeze protection. It is a part of the permanent non-safety-related loads and is powered from the diesel backed 480 Vac MCC through 480 V-208Y/120 V transformers and distribution panels. The staff finds the heat tracing system to be acceptable.

8.3.1.5 Containment Building Electric Penetrations

Individual electrical penetrations are provided for each electrical service level. Electrical circuits passing through electrical penetrations have primary and backup protective devices. These devices coordinate with the thermal capability curves (I^2t) of the penetration assemblies. The penetrations are rated to withstand the maximum short circuit currents available without exceeding their thermal limits, for at least longer than the field cables of the circuits. This ensures that the fault or overload currents are interrupted by the protective devices prior to a potential penetration failure. Penetrations are protected for the full range of currents up to the maximum short circuit current available. Primary and backup protective devices protecting Class 1E circuits are Class 1E in accordance with Institute of Electrical and Electronics Engineers (IEEE) Standard 741-1997, “Criteria for the Protection of Class 1E Power Systems and Equipment in Nuclear Power Generating Stations.” Primary and backup protective devices protecting non-Class 1E circuits are non-Class 1E. The staff notes that IEEE 741-1997 is not endorsed by a regulatory guide.

The electrical circuits passing through electrical penetrations are protected by coordinated primary and backup protective devices. The primary and backup protective devices protecting Class 1E circuits are in accordance with IEEE 317-1976, “Electric Protection Assemblies in Containment Structures for Nuclear Power Generating Stations,” which is endorsed by RG 1.63, “Electric Penetration Assemblies in Containment Structures for Nuclear Power Plants,” Revision 3. The design is, therefore, acceptable.

8.3.1.6 Grounding System

The AP1000 grounding system will comply with the guidelines provided in IEEE 665-1995, "Guide for Generating Station Grounding," and IEEE 1050-1996, "Guide for Instrumentation and Control Equipment Grounding in Generating Stations." Specifically, the grounding system consists of the following four subsystems:

(1) station grounding grid
(2) system grounding
(3) equipment grounding
(4) instrument and computer grounding

The station grounding grid subsystem consists of buried, interconnected bare copper conductors and ground rods forming a plant ground grid matrix. The subsystem will maintain a uniform ground potential and will limit the step-and-touch potentials to safe values under all fault conditions.

The system grounding subsystem will provide grounds of the neutral points of the main generator, main step-up transformers, auxiliary transformers, load center transformers, and onsite standby diesel generators. The main and diesel generator neutrals will be grounded through grounding transformers providing high-impedance grounding. The main step-up and load center transformer neutrals will be grounded solidly. The auxiliary (unit and reserve) transformer secondary winding neutrals will be resistance-grounded.

The equipment grounding subsystem will ground the equipment enclosures, metal structures, metallic tanks, ground bus of switchgear assemblies, load centers, MCCs, and control cabinets with ground connections to the station ground grid.

The instrument and computer grounding subsystem will ground plant instruments and computers through a separate radial grounding system consisting of isolated instrumentation ground buses and insulated cables. The radial grounding systems will be connected to the station grounding grid at only one point, and will be insulated from all other grounding circuits.

The final design of the grounding and the lightning protection system depends on the soil resistivity and lightning activity in the area. DCD Tier 2, Section 8.3.3 states that the COL applicant referencing the AP1000 certified design will address the design grounding and lightning protection. This is COL Action Item 8.3.1.6-1.

8.3.1.7 Lightning Protection

In accordance with the Lighting Protection Code, National Fire Protection Association (NFPA) 780-1997, "Standard for the Installation of Lightning Protection Systems," the lightning protection system, consisting of air terminals and ground conductors, will protect the containment/shield building, cooling towers, switchyard, and other exposed structures and buildings housing safety-related and fire protection equipment. In addition, lightning arresters will be provided in each phase of the transmission lines and at the high voltage terminals of the outdoor transformers. The isophase bus connecting the main generator, main transformer, and medium voltage switchgear will also be provided with lightning arresters. In addition, a surge suppressor will be provided to protect the plant instrumentation and monitoring system from lightning-induced surges in the signal and power cables connected to a device located outside.

Direct strike lightning protection for facilities is accomplished by providing a low-impedance path by which the lightning strike discharge can enter the earth directly. The direct strike lightning protection system (consisting of air terminals, interconnecting cables, down conductors to ground, and other components) will be provided external to the facility in accordance with the guidelines included in NFPA 780-1997. The system will be connected directly to the station ground to facilitate dissipation of the large current of a direct lightning strike. The lightning arresters and the surge suppressor connected directly to the ground provide a low-impedance path to ground for the surges caused or induced by lightning. Thus, damage to facilities and equipment resulting from a lightning strike is avoided.

The final design of direct lightning protection and the associated grounding depends on the lightning activity at the plant site and the soil resistivity of the ground. As discussed in Section 8.3.1.6 of this report, the COL applicant referencing the AP1000 certified design will address the design of its lightning protection system.

8.3.1.8 Raceway and Cable Installation

There are two non-safety-related load groups associated with different transformers, buses, and onsite standby diesel generators. No physical separation is required because these two ac load groups are non-Class 1E and non-safety-related. The power cable ampacities are in accordance with the Insulated Cable Engineers Association (ICEA) publications and the National Electric Code. The derating is based on the type of installation, the conductor and ambient temperature, the number of cables in a raceway, and the groupings of the raceways. A further derating of the cables is applied for those cables that pass through a fire barrier. The method of calculating these derating factors is determined from the ICEA publications and other applicable standards.

For circuits that are routed through conduit and partly through trays or underground ducts, the cable size is based on the ampacity in that portion of the circuit with the lowest indicated current carrying capacity.

In DCD Tier 2, Section 8.3.1.3.3, “Cable Derating and Cable Tray Fill,” the cable tray design is based on random cable fill of 40 percent of usable tray depth. The applicant has committed to analyze the tray fill if it exceeds the above stated maximum fill.

Separate raceways are provided for medium voltage power, low voltage power, and control, as well as instrumentation cables. Non-Class 1E raceways and supports, installed in seismic Category I structures, are designed and/or physically arranged so that an SSE could not cause unacceptable structure interaction or failure of seismic Category I components.

The raceway system for non-Class 1E ac circuits complies with IEEE 422-1986, “IEEE Guide for the Design and Installation of Cable Systems in Power Generating Stations,” with respect to installation and support of cable runs between electrical equipment, including physical protection. The staff notes that IEEE 422-1986 is not endorsed by a regulatory guide.

On the basis of the staff's review of the information provided, the staff considers that the raceway and cable installation description is adequate, and therefore, acceptable.

8.3.1.9 Conclusions

The applicant has specified appropriate design criteria for the non-Class 1E onsite ac power system. Because the passive safety systems do not require Class 1E ac onsite power, the staff concludes that the onsite power systems (except for the Class 1E batteries discussed below in Section 8.3.2 of this report) are acceptable.

8.3.2 Direct Current Power and Uninterruptible Power Systems

Regulatory Evaluation

The dc power systems include those dc power sources (and their distribution systems and auxiliary supporting systems) provided to supply motive or control power to safety-related equipment. The staff’s review covers the information, analyses, and referenced documents for the dc onsite power system. Acceptance criteria are based on GDC 17, as they relate to the capability of the onsite electrical power system to facilitate the functioning of structures, systems, and components (SCCs) important to safety. Specific review criteria are contained in SRP Sections 8.1 and 8.3.2, “D-C Power Systems (Onsite).”

Technical Evaluation

The dc power system consists of Class 1E and non-Class 1E dc power systems. Each system consists of ungrounded batteries, dc distribution equipment, and a UPS.

The Class 1E dc and UPS system supplies power for Class 1E equipment required for the plant instrumentation, control, monitoring, and other vital functions needed for plant safety. In addition, the Class 1E dc and UPS system powers the lighting in the MCR and in the remote shutdown area.

The Class 1E dc and UPS system also supplies power for the safe shutdown of the plant without the support of battery chargers, during a loss of all ac power sources coincident with a design-basis accident (DBA). The system is designed so that no single failure will result in a condition that will prevent the safe shutdown of the plant.

The non-Class 1E dc and UPS system provides power to the plant’s non-Class 1E control and instrumentation equipment and loads that are required for plant operation and investment protection, and to the hydrogen igniters located inside containment. Operation of the non-Class 1E dc and UPS systems is not required for plant safety.

8.3.2.1 Class 1E dc and UPS System

The AP1000 Class 1E dc and UPS system consists of Class 1E dc distribution, the Class 1E uninterruptible power system, and testing and inspection of the dc power system. The Class 1E dc and UPS system design was reviewed against GDC 2, "Design Bases for Protection Against Natural Phenomena," GDC 4, "Environmental and Missile Design Basis," GDC 17, GDC 18, and GDC 50, "Containment Design Basis," as listed in the SRP. GDC 5, "Sharing of Structures, Systems, and Components," is not applicable to the AP1000 design because this design is only for a single unit.

8.3.2.1.1 Class 1E dc Distribution

The Class 1E dc power system consists of four independent 125 V Class 1E dc safety system divisions (Divisions A, B, C, and D). Divisions A and D are each comprised of one battery bank, one switchboard, and one battery charger. Divisions B and C are each comprised of two battery banks, two switchboards, and two battery chargers.

A battery bank in each of the four divisions, designated as a 24-hour battery bank, is used to provide power to the loads required for the first 24 hours following a loss of all ac power sources concurrent with a DBA. The second battery bank in Divisions B and C, designated as a 72-hour battery bank, is used for loads requiring power for 72 hours following the same event. In the event of a LOOP coincident with a generator trip, ac power to the battery charger is provided from two separate non-Class 1E onsite standby diesel generators. Divisions A and C chargers receive ac power from one diesel generator, and Divisions B and D chargers from the second diesel generator. Provisions are also made to power Divisions B and C chargers from transportable ac generators during the post-72-hour period. No load shedding or load management program is needed to maintain power during the required 24-hour safety actuation periods.

In request for information (RAI) 435.015, the staff expressed a concern regarding the ability of the dc system to suppress voltage spikes that may result from surges caused by deenergized, highly inductive loads, since the battery charger is powered from the ac system. By letter dated October 2, 2002, the applicant responded that the dc system is protected from surges generated on the ac system by the isolation provided by the battery chargers and voltage regulating transformers. To further assure protection, metal oxide varistor surge suppressors are used at the input terminals to all battery chargers and inverters to minimize the potential for component damage resulting from electrical transients. The metal oxide varistor surge suppressor is safe to use. It does not emit toxic fumes upon failure and arcing or burning. On the dc system, inductive loads are limited to relay and motor starter coils. Surge suppression devices are installed across the coils to limit voltage spikes when the coils deenergize. In the ac system surge arresters are used in locations where switching or lightning transients may occur. In addition, surge suppressors are provided to protect the plant instrumentation and monitoring system from lightning-induced surges in the signal and power cables connected to devices located outside.

The Class 1E dc system is ungrounded. Thus, a single ground fault does not cause immediate loss of the faulted system. However, Class 1E detection with alarms is provided for each power division, so that ground faults can be located and removed before a second fault could disable the affected circuit.

Each Class 1E 24-hour and 72-hour battery charger is tested to verify its capability to provide power while maintaining the output voltage within the specified range. Each battery charger has an input ac and output dc circuit breaker for the purpose of power source isolation. Each battery charger prevents the ac supply from becoming a load on the battery due to power feedback (as a result of the loss of ac power to the chargers). Each battery charger has a built-in current limiting circuit, adjustable between 110 to 125 percent of its rating, to hold down the output current in the event of a short circuit or overload on the dc side. The output of the charger is ungrounded and filtered. The output float and equalizing voltages are adjustable.

The battery chargers have an equalizing timer and a manual bypass switch to permit periodic equalizing charges. Each charger is capable of providing continuous Class 1E loads while providing sufficient power to charge a fully discharged battery within a 24-hour period.

The AP1000 Class 1E 125 Vdc batteries are sized to meet the design requirements of their connected load, without the charger support, for the corresponding time periods of 24 and 72 hours. The batteries have been sized in accordance with IEEE 485-1997. The staff notes that IEEE 485-1997 is not endorsed by a regulatory guide. The staff considers that the governing factor for the AP1000 Class 1E battery size is the steady-state loading condition. The steady-state loads are required to operate for a long period of time (0 to 24 hours and 0 to 72 hours). Therefore, the staff considers the battery sizing acceptable.

Monitoring and Alarms

Each battery bank, including the spare, has a battery monitor system which detects battery open circuit conditions and monitors battery voltage. The battery monitor provides a trouble alarm locally and in the MCR. The battery monitors are not required to support any function.

The specific considerations regarding the monitoring of the dc power systems are derived from Section 7.4 of IEEE 946-1992, "IEEE Recommended Practice for the Design of DC Auxiliary Power Systems for Generating Stations." Although IEEE 946-1992 is not endorsed by a regulatory guide, the staff considers monitoring to be beneficial. In summary, these general considerations state that the dc systems (batteries, distribution system, and chargers) should be monitored to the extent that they can be shown to be ready to perform their intended functions. The recommended instruments, controls, alarms, and their locations are described below:

Instrument/Alarm/Control	Main Control Room	Local
Battery Current (Ammeter Charge/Discharge)		X
Battery Charger Output Current (Ammeter)		X
DC Bus Voltage (Voltmeter)		X
Battery Charger Output Voltage (Voltmeter)	X	

Instrument/Alarm/Control	Main Control Room	Local
Ground Detector (Voltmeter)	X	
DC Bus Undervoltage Alarm	X	
DC System Ground Alarm	X	
Battery Breaker/Switch Open Alarm	X	
Battery Charger Output Breaker Open Alarm	X	
Battery Charger DC Output Failure Alarm	X	
Battery Charger AC Power Failure Alarm	X	
Charger Low DC Voltage Alarm	X	
Charger High DC Voltage Shutdown Relay (opens main ac supply breaker to the charger)	X	
Battery Test Breaker Closed Alarm	X	X

Monitoring and alarming of dc current and voltages is through the plant control system, which includes a battery discharge rate alarm. The operating range for the safety-related dc power system is 105 to 140 Vdc. This voltage range envelopes the DBA conditions; the batteries have been sized to provide adequate voltage at the end of the battery duty cycle.

In RAI 435.006, the staff questioned whether the standard, molded-case ac breakers will be used in dc circuits because the dc interrupting rating will generally be less than the ac value. Many manufacturers do not publish dc application data for these breakers. By letter dated October 2, 2002, the applicant responded that the limited availability of molded-case breakers with a high dc interrupting rating is known in the industry. However, there are manufacturers who can supply molded case breakers with UL-listed interrupting ratings for dc circuits. The application of molded-case circuit breakers in the AP1000 dc distribution system is described below:

- The AP1000 design generally utilizes fusible disconnect switches in the Class 1E dc system. If a molded-case circuit breaker is used in a particular circuit, it will be sized to meet the dc interrupting rating specification. Proper documentation will be obtained to ensure that the molded-case breakers have adequate dc interrupting rating.

- The non-Class 1E dc power system has molded-case circuit breakers. These breakers will have UL-listed current interrupting ratings for dc applications.

The Class 1E dc switchboards employ fusible disconnect switches and have adequate short circuit and continuous current ratings. Fused transfer switch boxes, equipped with double pole, double throw transfer switches, are provided to facilitate battery testing and maintenance. The fuses are housed in the fused transfer switch boxes. To provide maximum protection coverage from short circuit, each fused transfer switch box is located as close to the battery terminals as possible. The fuses are sized in accordance with the criteria stated in Section 7.1 of IEEE 946-1992. The continuous current rating of the fuses is sufficiently high to prevent damage to the fuse element at the 1-minute current rating of the battery, and sufficiently low to ensure interruption of the short circuit current available from the battery at end-of-discharge voltage.

8.3.2.1.2 Class 1E Uninterruptible Power System

The Class 1E UPS provides power at 208/120 Vac to four independent divisions of Class 1E instrument and control power buses. Divisions A and D each consists of one Class 1E inverter with an instrument and control distribution panel and a Class 1E backup regulating transformer. The inverter is powered from the respective 24-hour battery bank. Divisions B and C each consist of two inverters, two instrument and control distribution panels, and a backup regulating transformer. One inverter is powered by the 24-hour battery bank and the other by the 72-hour battery bank. Under normal operation, the Class 1E inverters receive power from the associated battery bank. If an inverter is inoperable, or the Class 1E 125 Vdc input to the inverter is unavailable, the power is transferred automatically to the backup ac source by a static transfer switch, featuring a make-before-break contact arrangement. The backup power is received from the diesel generator backed non-Class 1E 480 Vac bus through the Class 1E regulating transformer. In addition, a manual mechanical bypass switch is provided to allow connection of a backup power source when the inverter is removed from service for maintenance.

The Class 1E dc and UPS system is designed to accommodate component failures, such as the loss of a battery charger, a battery, or an inverter, without the loss of power to either the dc bus or the ac instrumentation and control power bus. In RAI 435.008, the staff expressed a concern that failures of the UPS system constitute one of the main causes of forced plant outages and requested the applicant to discuss the design aspects that will ensure that the failure or unavailability of a single battery, battery charger, or inverter will not result in a plant trip. By letter dated October 2, 2002, the applicant responded that a failure or the unavailability of a single safety-related battery, battery charger, or inverter will not result in a plant trip or a forced outage. DCD Tier 2, Section 8.3.2, “DC Power Systems,” provides a description of the dc power systems. The dc power systems include a spare Class 1E battery bank with a spare battery, battery charger, and permanently installed cable connections that allow the spare bank to be connected to the affected bus by a plug-in, twist-lock disconnect. The spare bank can be aligned to either the Class 1E or the non-Class 1E dc power system, if component failures occur.

Following a loss of either a Class 1E or a non-Class 1E battery charger, which is normally providing power to the associated dc bus, the battery would immediately supply the affected bus, maintaining continuity of power to it. Following a loss of either a Class 1E or a non-Class 1E battery, the battery charger would continue to supply power to the dc bus. With the loss of either a battery charger or a battery, continuity of power to the associated dc bus is maintained. Therefore, there is no affect on plant operation since the spare battery can be aligned while the faulty component is repaired. Following the loss of either a Class 1E or a non-Class 1E inverter, the associated dc bus remains energized and the dc loads are not affected. The 208Y/120 Vac I&C power bus associated with the failed inverter remains continuously energized.

Each UPS includes an inverter and a Class 1E backup voltage regulating transformer that can supply the associated I&C bus, if the inverter fails. The UPS includes a static transfer switch that automatically transfers the bus to the regulated power source if power is unavailable from the inverter. A manual mechanical bypass switch is also included in the UPS to provide a second connection for the bus to the backup regulated power source when the inverter is removed from service for maintenance. Therefore, with a failure of a single battery charger or a single battery, power is continuously maintained to the dc buses. With a failure of an inverter, power to the I&C power bus is automatically transferred to a Class 1E regulated backup power source. With a single failure or the unavailability of these components, the associated buses remain energized, thereby preventing a plant trip or forced outage. This meets the single failure criterion. Therefore, the staff finds this acceptable.

In a RAI 435.010, the staff requested information from the applicant regarding the possibility of age-related failures of inverters and chargers, especially with an increase in ambient temperatures being considered as the main cause of age-related failures (particularly for capacitors, transformers, and semiconductors). The applicant was asked to describe the conservatism included in the AP1000 design with respect to temperature margins, and whether any forced air cooling for the battery chargers is required. By letter dated October 2, 2002, the applicant responded that the Class 1E and non-Class 1E inverters and battery chargers (UPS equipment) are located in a controlled environment. The room ambient temperature is maintained between 19 °C (66.2 °F) and 23 °C (73.4 °F) for the Class 1E equipment and between 10 °C (50 °F) and 40 °C (104 °F) for the non-Class 1E UPS equipment. The UPS equipment is rated for continuous operation at an ambient temperature of 40 °C (104 °F). In addition, the temperature-sensitive components such as capacitors, transformers, and semiconductors, used in the UPS equipment are designed to continuously withstand higher temperatures of about 60 °C (140 °F) to 70 °C (158 °F). In addition, Class 1E electrical components are environmentally qualified. Therefore, considering the conservative temperature margins provided in the AP1000 design, an age-related failure of the UPS equipment is not expected.

Air cooling is provided by the nuclear island nonradioactive ventilation system for Class 1E UPS equipment located in the auxiliary building. This system is described in DCD Tier 2, Section 9.4.1, “Nuclear Island Nonradioactive Ventilation System.” The non-Class 1E UPS equipment is located in the annex building. Air cooling is provided in the annex building by the annex building nonradioactive ventilation system which is described in DCD Tier 2, Section 9.4.2, “Annex/Auxiliary Buildings Nonradioactive HVAC System.” Therefore, based on the conservative temperature margins provided in the AP1000 design, an age-related failure of the UPS equipment is not expected. The staff finds the conservatism in the design to be acceptable.

In a RAI 435.014, the staff requested clarification as to whether the AP1000 design acceptably addresses total harmonic distortion (THD) for nonlinear loads. The loads used for digital control power supplies and computers in the AP1000 are inherently nonlinear in nature. Also, variable speed drive systems and fluorescent lighting ballasts introduce harmonics into the plant distribution system. By letter dated October 2, 2002, the applicant responded that THD due to nonlinear loads has been addressed in the AP1000 design. The UPS inverters have harmonic filters designed specifically to reduce the effects of large third, fifth, seventh, and higher-order harmonics that may result from anticipated 100 percent nonlinear loads. To provide high-quality power from the UPS system, the inverters are specified to power loads with a crest factor of 2 or higher (ratio of peak to root mean square [rms] value). The variable speed drives used for the RCPs have special filters to eliminate the introduction of harmonics into the distribution system. Also, the battery chargers are furnished with output filtering to limit ripple currents feeding into the dc power supply for the inverters. The applicant has shown that the issues associated with THD have been adequately addressed. Therefore, the staff considers this to be resolved.

The applicant performed a FMEA for the Class 1E dc and UPS system. In the event of a LOOP coincident with a generator trip, ac power to the battery charger is provided from two separate non-Class 1E onsite standby diesel generators. The Class 1E battery chargers and Class 1E regulating transformers are designed to limit the input ac current to an acceptable value under faulted conditions on the output side. Circuit breakers exist at the input and output sides for protection and isolation. The circuit breakers are coordinated and periodically tested to verify their current-limiting characteristics.

The four divisions are completely independent and located in separate rooms, have no shared equipment, and cannot be interconnected. Their circuits are routed in dedicated, physically separated raceways. This electrical and physical separation prevents the failure or unavailability of a single battery, battery charger, or inverter from adversely affecting a redundant division. The battery monitoring system detects battery open circuit conditions and monitors battery voltage. The Class 1E dc system is ungrounded. Thus, a single ground fault does not cause immediate loss of faulted system. A spare battery bank and charger enables testing, maintenance, and equalization of battery banks offline. This configuration provides the capability for each battery bank or battery charger to be separately tested and maintained (including battery discharge tests, battery cell replacement, battery charger replacement) during plant operation.

The AP1000 design uses battery monitors. These monitors continuously monitor the condition of the battery by measuring intercell resistance to provide advance indication of a maintenance requirement. Also, the batteries are in a controlled environment during normal operation. The controlled environment helps eliminate the possibility of a common mode failure caused by a high room ambient temperature.

8.3.2.1.3 Testing and Inspection of the dc Power System

GDC 18 requires that electric power systems important to safety shall be designed with the following capabilities:

- the ability to permit appropriate periodic inspection and testing of important areas and features (such as wiring, insulation, connections, and switchboards) in order to assess the continuity of the systems and the condition of their components

- the ability of periodically test the operability and functional performance of the components of the systems

- the ability to periodically test the operability of the systems as a whole (under conditions as close to design as practical) and the full operation sequence that brings the systems into operation

The applicant stated that components of the 125 Vdc system undergo periodic tests to determine the condition of the system. Batteries are checked for electrolyte level, specific gravity, and cell voltage. The surveillance testing of the Class 1E 125 Vdc system is performed as required by the AP1000 DCD Tier 2, Chapter 16, “Technical Specifications.” The staff concludes that the Class 1E 125 Vdc electric power system is periodically tested and inspected in accordance with GDC 18 and is, therefore, acceptable.

8.3.2.1.4 Conclusions

The applicant has met the requirements of GDC 2 with respect to the ability of the SSCs of the Class 1E dc and UPS system to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, and floods. The Class 1E dc and UPS system and components are located in seismic Category I structures which provide protection from the effects of tornadoes, tornado missiles, and floods. In addition, the Class 1E dc and UPS system and components have a quality assurance designation as “Class 1E.”

The applicant has met the requirements of GDC 4 with respect to the ability of the SSCs of the Class 1E dc and UPS system to withstand the effects of missiles and environmental conditions associated with normal operation and postulated accidents based on adequate plant design and equipment qualification program.

GDC 5 is not applicable to the AP1000 design because this design is only for a single unit.

The applicant has met the requirements of GDC 17 with respect to the Class 1E dc and UPS system's (1) capacity and capability to permit functioning of SSCs important to safety, (2) the independence and redundancy to perform its safety function assuming a single failure, and (3) provisions to minimize the probability of losing electric power from any of the remaining supplies as a result of, or coincident with, the loss of power generated by the nuclear power unit or the loss of power from the transmission network.

The applicant has met the requirements of GDC 18 with respect to the Class 1E dc and UPS system being designed to be testable during operation as well as during shutdown.

The applicant has met the requirements of GDC 50 with respect to penetrations containing circuits of the Class 1E dc and UPS system. Containment electrical penetrations have been designed to accommodate, without exceeding their design leakage rate, the calculated pressure and temperature conditions resulting from any loss-of-coolant accident (LOCA) concurrent with the maximum short circuit current versus time condition that could occur given, single random failures of circuit overload protective devices.

Therefore, the staff concludes that the plant design is acceptable.

8.3.2.2 Physical Independence of Redundant Circuits

There are four safety-related separation groups for the cable and raceway system (Groups A, B, C, and D). Separation Group A contains safety-related circuits from Division A. Similarly, separation Groups B, C, and D contain safety-related circuits from Divisions B, C, and D, respectively. There is also a Group N which contains non-safety-related circuits. Cables of each separation group are run in separate raceways and are physically separated from cables of other separation groups.

Group N raceways are separated from safety-related Groups A, B, C, and D. Raceways from Group N are routed in the same areas as the safety-related groups according to spatial separation as described in RG 1.75, "Physical Independence of Electric Systems," which endorses IEEE 384-1974, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." The applicant has applied IEEE 384-1974 with the following exceptions:

- Within the MCR and remote shutdown area (non-hazard areas), the minimum vertical separation for an open cable tray is 7.6 centimeters (cm) (3 in.) and the minimum horizontal separation is 2.54 cm (1 in.).

- Within general plant areas (limited hazard areas), the minimum vertical separation is 0.3 m (12 in.), and the minimum horizontal separation is 0.15 meter (m) (6 in.) for the open cable trays with low voltage power circuits for cable sizes <2/0 American Wire Gauge. For configurations that involve exclusively limited energy content cables (I&C), these minimum distances are reduced to 7.65 cm (3 in.) and 2.54 cm (1 in.), respectively.

- Within panels and control switchboards, the minimum horizontal separation between components or cables of different separation groups (both field-routed and vendor-supplied internal wiring) is 2.54 cm (1 in.), and the vertical separation distance is 0.15 m (6 in.).

- For configurations involving an enclosed raceway and an open raceway, the minimum vertical separation is 2.54 cm (1 in.), if the enclosed raceway is below the open raceway.

Section 5.1.1.2 of IEEE 384-1974 states that the minimum separation distance can be established by analysis of the proposed cable installation. This analysis shall be based on the tests performed to determine the flame retardant characteristics of the proposed cable installation, considering features such as cable insulation and jacket materials, cable tray fill, and cable tray arrangement. The applicant has established the minimum separation distances by performing an analysis of the proposed cable installation. This analysis is based on 10 tests performed and the findings published in the IEEE Transactions on Energy Conversion, Volume 5, No. 3, September 1990, titled, "Cable Separation—What Do Industry Testing Programs Show?" These findings were also published by the IEEE Working Group on Independence Criteria, SC-6.5, of the Nuclear Power Engineering Committee. The staff reviewed the results of the 10 tests and found them acceptable. Therefore, the staff finds the lesser distances used by the applicant in its design to be acceptable.

Non-Class 1E circuits are electrically isolated from Class 1E circuits by isolation devices and are physically separated from Class 1E circuits in accordance with the above separation criteria. Class 1E circuits from different separation groups are electrically isolated by isolation devices, shielding, and physical separation, in accordance with RG 1.75 for circuits in raceways. Non-Class 1E raceways and supports installed in seismic Category I structures are designed and/or physically arranged so that an SSE could not cause failure of seismic Category I components.

Power and control cables are installed in conduits or ventilated bottom trays (ladder type). Solid tray covers are used in outdoor locations. Instrumentation cables are routed in conduits or solid bottom cable trays with solid tray covers. Separate trays are provided for each voltage level—6.9 kV, low voltage power (480 Vac, 120 Vac, 125 Vdc), high-level signal and control (120 Vac, 125 Vdc), and low-level signal (instrumentation). Cable trays are physically arranged from top to bottom, in accordance with the function and voltage class of the cables, and with the highest voltage at the top. Vertically stacked trays are arranged from top to bottom with a minimum of 12 inches (0.3 m) vertical spacing maintained between trays of different service levels within the stack.

Raceways installed in seismic Category I structures have seismically designed supports, or are shown not to affect safety-related equipment should they fail. Conduits are attached to seismic Category I equipment with flexible type connections.

Where hazards to safety-related raceways are identified, a minimum separation is maintained between the break and/or missile source and any safety-related raceway. Alternatively, a barrier designed to withstand the effects of the hazard is placed to prevent damage to the raceways of redundant systems. Spacial separation is provided where redundant circuits, devices, or equipment (different separation groups) are exposed to the same external hazards. Otherwise, qualified barriers are installed.

The staff finds that the physical independence of the redundant circuits meets RG 1.75 with the exceptions discussed above. The distances specified in the exceptions to RG 1.75 are acceptable based on the staff's review of the 10 tests. Therefore, the physical independence of the redundant circuits is acceptable.

8.3.2.3 Non-Class 1E dc and UPS System

The non-Class 1E dc and UPS system consists of the dc electric power supply and distribution equipment that provide dc and uninterruptible ac power to the plant non-Class 1E dc and ac loads (that are needed for plant operation and investment protection) and to the hydrogen igniters located inside containment. The non-Class 1E dc and UPS system consists of two subsystems representing two separate power trains. The subsystems are located in separate rooms. Each subsystem consists of separate dc distribution buses, but these can be connected by a normally open circuit breaker. Each dc subsystem includes battery chargers, batteries, dc distribution equipment, and associated monitoring and protective devices.

Direct current buses 1, 2, and 3 provide 125 Vdc power to the associated inverter units that supply the ac power to the non-Class 1E UPS system. An alternative regulated ac power source for the UPS buses is supplied from the associated regulating transformers. Bus 4 supplies large dc motors and other dc power loads, but not inverter loads.

A 480 Vac distribution system backed by the onsite standby diesel generator provides the normal ac power to the battery chargers. The batteries supply the dc power in case the battery chargers fail to supply the dc distribution bus system loads. The batteries are sized to supply the system loads for a period of at least 2 hours after loss of all ac power sources. Each non-Class 1E dc distribution subsystem bus has provisions to allow connection of a spare non-Class 1E battery charger, in case its non-Class 1E battery charger is unavailable because of maintenance, testing, or failure. There are also provisions for the non-Class 1E dc system to use the Class 1E spare battery bank as a temporary replacement for any non-Class 1E battery bank. In this configuration, the spare Class 1E battery bank does not simultaneously supply Class 1E safety loads. Additionally, the design includes two current interrupting devices to preserve the spare Class 1E battery integrity should the non-Class 1E bus experience an electrical fault. Therefore, the Class 1E spare battery would not be degraded.

The non-Class 1E 125 Vdc system provides dc and UPS to the plant’s non-Class 1E dc and ac loads that are needed for plant operation and investment protection. The provision of two separate current interrupting devices helps to ensure the independence of the Class 1E dc system from faults or failures in the non-Class 1E systems, and is therefore acceptable.

8.4 <u>Other Electrical Features and Requirements for Safety</u>

The staff reviewed certain safety-related electrical features of the AP1000 design to determine whether they are implemented in accordance with the applicable criteria set forth in Section 8.1 of this report.

8.4.1 Containment Electrical Penetrations

The applicant stated that the penetrations conform to the same functional service level as the cables (e.g., low-level instrumentation is separated from power and control penetrations). Individual electrical penetrations are provided for each electrical service level, and are arranged physically from top to bottom in accordance with the function and voltage class of the cables. For modular type penetrations (three penetration modules in one nozzle), the applicant has assigned the following:

- one module for low voltage power
- one module for 120 Vac/125 Vdc control and signal
- one module for instrumentation signal

Penetrations carrying medium voltage power cables have thermocouples to monitor the temperature within the assembly at the spot expected to have the hottest temperature. Electrical circuits passing through electrical penetrations have primary and backup protective devices. These devices are to be selected to coordinate with the thermal capability (I^2t) of the penetration assemblies. The applicant stated that the penetrations can withstand the maximum short circuit currents available either continuously, without exceeding their thermal limit, or at least longer than the field cables of the circuits. Therefore, the faults or overload currents are interrupted by the protective devices before a potential failure of a penetration. Penetrations are protected for the full range of current up to the maximum short circuit current available.

The containment electrical penetration assemblies for the AP1000 are designed to withstand, without loss of mechanical integrity, the maximum available fault current for a sufficient period of time to allow backup circuit protection to operate, assuming a failure of the primary protective device. This is in accordance with IEEE 317-1983, “Electrical Penetration Assemblies in Containment Structures for Nuclear Power Generating Stations,” as augmented by the recommendations of RG 1.63, Revision 3. Primary and backup protective devices protecting Class 1E circuits are Class 1E and are coordinated. DCD Tier 2, Section 8.3.3 states that the COL applicants referencing the AP1000 certified design will address the provisions for periodically testing the penetration protection devices. This is COL Action Item 8.4.1-1.

8.4.2 Reactor Coolant Pump Breakers

The RCPs are powered from the four switchgear buses located in the turbine building. One RCP is powered by each bus. Variable speed drives are provided for RCP startup. Each RCP is powered through two Class 1E circuit breakers connected in series. These are the only Class 1E circuit breakers used in the main ac power system for the specific purpose of satisfying the safety-related tripping requirements of these pumps. This ensures that the RCPs are tripped before the passive systems start.

The RCP trip function is a part of the engineered safeguards needed to respond to a design-basis LOCA, and, as a result, are implemented with Class 1E circuit breakers. Therefore, the staff finds the provision of two Class 1E circuit breakers for each RCP to be acceptable since they will allow the operation of the passive systems as designed.

8.4.3 Thermal Overload Protection Bypass

Motor-operated valves, with thermal overload protection devices for the valve motors, are used in safety systems and their auxiliary supporting systems. Operating experience has shown that indiscriminate application of thermal overload protection devices to the motors associated with these valves could result in a needless hindrance to the successful completion of safety-related functions. RG 1.106, “Thermal Overload Protection for Electric Motors on Motor-Operated Valves” (November 1975), recommends bypassing thermal overload devices during accident conditions (Regulatory Position C.1), or properly selecting the setpoint for the thermal overloads in a manner that precludes spurious trips (Regulatory Position C.2). Westinghouse Topical Report WCAP-15799, Revision 1, “AP1000 Conformance with SRP Acceptance Criteria,” states that the AP1000 design will comply with Regulatory Position C.1 of RG 1.106. The only safety-related electric motor operated valves are dc valves. For non-Class 1E valve motor operators, the thermal overload protection will remain in service at all times. The staff finds this is acceptable.

8.4.4 Power Lockout to Motor-Operated Valves

BTP ICSB 18 (PSB), "Application of the Single-Failure Criterion to Manually-Controlled Electrically-Operated Valves," states that all valves that require power lockout to meet the single failure criterion in the fluid systems, and their required positions, be listed in the technical specifications. It also states that the position indications for these valves should meet the single failure criterion. With respect to the power lockout to the motor-operated valves, this position establishes the acceptability of disconnecting power to electrical components of a fluid system as one means of designing against a single failure that might cause an undesirable component action. DCD Tier 2, Section 7.6, "Interlock Systems Important to Safety," identified the following valves which require removal of power consistent with the guidelines of BTP ICSB-18:

- accumulator isolation valves and in-containment refueling water storage tank discharge valve

- passive residual heat removal heat exchanger inlet isolation valve

BTP ICSB-18, Item B-4, states that these valves, which have the electrical power removed to meet the single failure criterion, should have redundant position indication in the MCR, and the position indication system should, itself, meet the single failure criterion. The applicant has provided such indication in the MCR and the remote shutdown panel. Each of the two position sensors is powered from a different non-Class 1E power source. The power lockout to motor-operated valves meets BTP ICSB-18, Item B-4, and is therefore acceptable.

8.4.5 Submerged Class 1E Electrical Equipment as a Result of a Loss-of-Coolant Accident

DCD Tier 2, Section 3.11, "Environment Qualification of Mechanical and Electrical Equipment," discusses the environmental qualification of electrical and mechanical equipment. DCD Tier 2, Table 3.11-1 lists the safety-related electrical and mechanical equipment. The applicant stated that equipment will be qualified for submergence resulting from flooding/wetting. As an alternative to protecting the equipment, the equipment will be evaluated to show that failure of the equipment because of flooding/wetting is acceptable since its safety-related function is not required, or has otherwise been accomplished.

Environmental qualification of electrical equipment is further addressed in Section 3.11 of this report.

8.5 Compliance with Regulatory Issues

8.5.1 Generic Issues and Operational Experience

The staff evaluated the following generic issues and operational experience (bulletins and generic letters). The staff used Topical Report WCAP-15800, Revision 3, "Operational Assessment for AP1000," issued July 2004, and NUREG-0933, "A Prioritization of Generic Safety Issues," to determine the generic issues and operational experience relevant to the AP1000 design.

- A-24, "Qualification of Class 1E Safety-Related Equipment"
- A-25, "Non-Safety Loads on Class 1E Power Sources"
- A-35, "Adequacy of Offsite Power Systems"
- A-44, "Station Blackout"
- B-53, "Load Break Switch"
- B-56, "Diesel Reliability"
- 128: "Electrical Power Reliability"
- II.E.3.1, "Emergency Power Supply for Pressurizer Heaters"
- II.G.1, "Power Supplies for Pressurizer Relief Valves, Block Valves, and Level Indicators"
- BL 80-20, "Failures of Westinghouse Type W-2 Spring Return to Neutral Control Switches"
- GL 80-013, "Qualification of Safety-Related Equipment"
- GL 80-016, "IEB 79-01b Environmental Qualification of Class 1E Equipment"
- GL 80-035, "Effect of a dc Power Supply Failure on ECCS Performances"
- GL 80-082, "IEB 79-01b, Supplement 2, Environmental Qualification of Class 1E Equipment"
- GL 82-09, "Environmental Qualification of Safety-Related Electrical Equipment"
- GL 84-24, "Certificate of Compliance to 10 CFR 50.49, Environmental Qualification of Equipment Important to Safety"

- GL 86-15, “Information Relating to Compliance With 10 CFR 50.49, ‘Environmental Qualification of Equipment Important to Safety for Nuclear Power Plants’”

- GL 88-07, “Modified Enforcement Policy Relating to 10 CFR 50.49, ‘Environmental Qualification of Electrical Equipment Important to Safety for Nuclear Power Plants’”

- GL 88-15, "Electrical Power Systems —Inadequate Control Over Design Process”

The generic issues and operational experience listed above are discussed in Chapter 20 of this report.

8.5.2 Advanced Light-Water Reactor Certification Issues

The following paragraphs discuss the policy, technical, and licensing issues pertaining to passive plant designs that relate to the electrical portion of the AP1000 design.

8.5.2.1 Station Blackout

The requirements of 10 CFR 50.63, “Station Blackout,” state that all nuclear power plants must have the capability to withstand a loss of all ac power for an established period of time, and to recover therefrom. The AP1000 design minimizes the potential risk contribution of a station blackout (SBO) by not requiring ac power sources for design-basis events. Safety-related systems do not need non-safety-related ac power sources to perform safety-related functions. The AP1000 safety-related passive systems automatically establish and maintain safe-shutdown conditions for the plant following design-basis events, including an extended loss of ac power sources. The passive systems can maintain these safe-shutdown conditions after design-basis events for 72 hours, without operator action, following a loss of both onsite and offsite ac power sources. DCD Tier 2, Section 1.9.5.4, “Additional Licensing Issue,” provides additional information on long-term actions following an extended SBO beyond 72 hours.

The AP1000 design also includes redundant, non-safety-related, onsite ac power sources (diesel generators) to provide electrical power for non-safety-related active systems that provide a defense-in-depth function.

The following AP1000 design features mitigate the consequences of a SBO:

- a full load rejection capability to reduce the probability of loss of onsite power

- safety-related passive residual heat removal heat exchanger

- safety-related passive containment cooling

- bleed and feed capability, using the safety-related automatic depressurization system in conjunction with the water available from the core makeup tanks, accumulators, and in-containment refueling water storage tank

- class 1E batteries sized for 72 hours of operation under SBO conditions

- RCPs without shaft seals

- passive cooling for the rooms containing equipment assumed to operate during SBO conditions (the protection and safety monitoring system cabinet rooms and the MCR) so that this equipment continues to operate for 72 hours

The staff reviewed the applicant's submittal and Section 5, “Loss of All AC Power,” of Topical Report WCAP-15985, Revision 2, “AP1000 Implementation of the Regulatory Treatment of Non-Safety-Related Systems Process,” dated August 2003 and concludes that no installed non-safety-related systems, structures, and components are relied upon to meet the requirements of 10 CFR 50.63. The staff concludes that the safety-related passive systems are capable of withstanding a loss of all ac power for 72 hours. Therefore, the AP1000 design meets the requirements of 10 CFR 50.63 for 72 hours.

8.5.2.2 Electrical Distribution

The Commission approved the following recommendations in SECY-91-078 for plant designs:

- An alternative offsite power source will be available for non-safety-related loads, unless the design margins for loss of non-safety-related loads are no more severe than turbine-trip-only events in current plants.

- At least one offsite circuit to each redundant safety division will be supplied directly from offsite power sources, with no intervening non-safety-related buses.

The AP1000 design does not have to meet SECY-91-078 because the design does not rely on active systems for safe shutdown.

8.5.2.3 Regulatory Treatment of Non-Safety Systems

In SECY-95-132, “Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems (RTNSS) in Passive Plant Designs,” the NRC set forth policy regarding those systems in passive light-water reactors that are designated non-safety-related, but that may have a significant role in accident and consequence mitigation. The basis for selecting risk-important non-safety systems for the AP1000 is evaluated in WCAP-15985, Revision 2. The non-safety-related active systems in the AP1000 design provide defense-in-depth functions and supplements the capability of the safety-related passive systems. The process of identifying regulatory oversight on non-safety-related systems is referred to as RTNSS.

The ac power from the diesel generators is required to power the normal residual heat removal system (RNS) and to provide a means of supplying power to post-accident monitoring and the input ac power for the Class 1E dc battery chargers. The RNS provides a non-safety-related means to inject water into the reactor coolant system (RCS), following automatic depressurization system actuation in modes 1, 2, 3, and 4. The availability controls require that the ac power supply function be available in modes 1, 2, 3, and 4, when the RNS injection and projection and monitoring system actuation are more risk important.

The ac power is required to power the RNS and its required support systems. The RNS provides a non-safety-related means to normally cool the RCS during shutdown operations. The availability controls require that one offsite and one onsite ac power supply should be available during modes 5 and 6 with reduced inventory, when the loss of RNS cooling is important. The offsite power source is available through the transmission switchyard and either the main step-up transformer/unit auxiliary transformer or the reserve auxiliary transformer. The onsite power source is available from one of the two diesel generators. If both of these ac power sources are not available, the plant should not enter reduced inventory conditions.

The non-Class 1E dc and UPS systems are important for the diverse actuation system (DAS), based on 10 CFR 50.62, “Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants,” and to support engineered safety features actuation (ESFA), based on providing margin in the probabilistic risk assessment sensitivity performed. The availability controls require that the non-Class 1E dc and UPS system be available to the DAS sensors, DAS actuation, and the devices which control the actuated components in mode 1 for DAS ATWS mitigation function, and in modes 1, 2, 3, 4, 5, and 6 for DAS ESFA.

The availability controls require that one ancillary diesel generator, and its fuel oil storage tank, be available during all modes of plant operation. After 72 hours, ancillary diesel generators will power the MCR and I&C room ancillary fans, the PCS recirculation pumps, and MCR lighting.

Therefore, the applicant has provided availability controls for the electrical areas that are RTNSS important and has included these controls into the DCD and in the design certification rule to make the commitment binding on the COL applicant. Unlike the current generation of light-water reactors, the AP1000 uses passive safety systems that rely exclusively on natural forces such as gravity and stored energy to provide water for core and containment cooling. These passive systems do not include active equipment, such as pumps.

For the AP1000 design, the active systems are designated as non-safety-related systems. The non-safety-related systems in the AP1000 design provide defense-in-depth functions and supplement the capability of the safety-related passive systems. Thus, the staff and the industry have defined a process to evaluate the importance of the non-safety-related systems, and for maintaining regulatory oversight of these active systems in the AP1000 design.

The staff reviewed the RTNSS process and finds it acceptable. For an additional discussion on RTNSS refer to Chapter 22 of this report.