section C.2 with regard to provisions for decontamination is provided in Section 12.3.1.

12. The safety-related components and systems of the FPCPS are not shared among nuclear power units (GDC 5).

13. Designed to provide acceptable performance for the environments anticipated under normal, testing, and design basis conditions in compliance with the requirements of 10 CFR 50.49.

14. Monitoring capability provides on-demand indication of SFP level independent of AC and DC normal and emergency power sources.

9.1.3.2 System Description

9.1.3.2.1 General Description

The FPCPS system is described in following four sections:

- Fuel Building and Reactor Building pools.
- Fuel pool cooling system.
- SFP makeup capability.
- Fuel pool purification system.

9.1.3.2.2 Fuel Building and Reactor Building Pools

The Fuel Building pool (see also the description of the Fuel Building in Section 3.8.4 and the Spent Fuel Storage Facility in Section 9.1.2.2.2) includes the following three compartments:

- The Fuel Building Transfer Compartment is used for transfer of used or new fuel between the Fuel Building and the Reactor Building. This compartment is filled from the in-containment refueling water storage tank (IRWST) before refueling.
- The Cask Loading Pit is filled with water when spent fuel transfer from the pool is required. The water needed to fill this compartment is stored in the Fuel Building Transfer Compartment.
- The SFP is dedicated to the storage and cooling of the spent fuel.

The Reactor Building pool (see also the description of the Reactor Building in Section 1.2 and Section 3.8) includes the following four compartments:

- The Reactor Building transfer compartment is connected to the Fuel Building Transfer Compartment by a transfer tube (see Section 9.1.4), and is used for transfer of used or new fuel between the Fuel Building and the Reactor Building.

2. If the surge tank level drops below the MIN3 setpoint, the leak may be located in safety-related piping on the common header. The common headers are then isolated by closing of the switchover valves of the faulted train. The goal of this actuation is to provide availability of the train for its SIS users.

3. If the surge tank level continues to decrease below the MIN4 setpoint after the switchover valves are closed, the leak is located on the corresponding train. After reaching level MIN4, the associated CCWS train pump is tripped.

Dedicated Trains

In case of a pipe break, the dedicated CCWS surge tank pressure will decrease and the makeup pump will automatically start to maintain the pressure. If the water leak is greater than the capacity of the makeup pump to replace, a low level is reached in the tank, at which point the tank is automatically isolated to prevent nitrogen injection into the pump suction piping. The train pumps are correspondingly tripped and the train is unavailable.

Loss of one ESWS Train

CCWS Safety-Related Trains

In case of loss of one ESWS ~~or CCWS~~ train, an automatic backup switchover is performed to allow the cooling of the common headers using the available train. In case of a loss of an ESWS train, the corresponding CCWS train can be kept in operation supplying its safety users (SIS users) so long as the CCWS operating temperature is lower than 100.4°F, the maximum operating temperature for safety users.

Dedicated Train

The dedicated CCWS train is cooled by the dedicated ESWS train. In case of a loss of the dedicated ESWS train, the associated dedicated CCWS train is also lost.

Loss of a CCWS train

CCWS Safety-Related Trains

In case of loss of one CCWS train, an automatic backup switchover is done to allow the cooling of the common a or b headers (or both) with the available train. The restoration of cooling to the "a" headers is a manual sub-function of the automatic backup switchover.

Dedicated Train

In case of a loss of the dedicated CCWS train, the entire SAHRS cooling chain is lost.

Train automatic backup switchover consists of:

- Close switchover valves (KAA10/20/30/40 AA006/010) on the initial train and open LHSI heat exchanger isolation valve (KAA12/22/32/42 AA005).
- Open common 1.b (2.b) switchover valves (KAA10/20/30/40 AA006/010) on the on-coming train.
- Start CCWS pump (KAA10/20/30/40 AP001) on the on-coming train.

The on-coming train common .a sub-header switchover valve may then be manually opened. The functional logic is shown on Figure 7.3-33.

Emergency CCWS Temperature Control

An open CCWS heat exchanger bypass line can cause CCWS temperature to be greater than 100.4°F.

To prevent this condition, the bypass control valve of the CCWS heat exchanger (KAA10 AA112) is automatically stepped closed in approximate 10 percent increments when the heat exchanger outlet is near the high temperature threshold (MAX1). The valve is stepped closed until MAX1 is cleared.

This temperature control function is required during all plant modes of operation, when the CCWS (KAA10/20/30/40) is energized. The functional logic is shown on Figure 7.3-34.

Emergency Leak Detection Sequence

Leakage can occur in a CCWS train, which leads to a loss of system fluid and consequently in a drop in the CCWS level in the corresponding surge tank.

The following leakage detection sequence is initiated when the surge tank level is less than the MIN2 set point:

- The common user automatic and normal switchover sequence is inhibited to avoid the transfer of the faulted piping on the associated train. The non-safety-related branches are isolated by fast closing valves if there is a flow mismatch between the inlet and outlet of the users supply and return lines.

If the surge tank level continues to decrease to less than the MIN3 setpoint, the common headers are isolated by closure of the switchover valves (KAA10/20/30/40 AA006/010/032/033) and the switchover sequence is prohibited.

If the surge tank level continues to decrease to less than MIN4 set point, the associated CCWS train pump is tripped and the common user sets switchover sequence function is unlocked to allow supplying of the common users by the opposite train capable of

supplying the common header. The DWDS supply isolation valve (KAA10/20/30/40 AA027) is also closed in order to avoid DW water supply to a train with a leak.

The surge tank level is detected by two redundant analog level measurements. The functional logic is shown on Figure 7.3-35.

Switchover Valves Leakage or Failure

In the event of a switchover valve seat leakage or failure and depending upon the difference in pressure between the two CCWS trains, a water transfer could occur. If the water transfer leads to a MAX2 surge tank level in one of the two associated trains and a MIN3 surge tank level on the other, the common users are automatically isolated from the safety trains. This action allows both trains to perform their main safety-related function. The function logic is shown on Figure 7.3-36.

Safety Chilled Water Condenser Supply Water Flow Control

The SCWS chillers of Trains 2 and 3 are ~~permanently~~ cooled by one of two associated CCWS common headers. They are isolable from all other associated Common header users by means of manual valves ((KAA22/32AA003/004). They are fitted with a three-way flow control valve (KAA22/32AA101) that is controlled by the chiller condenser refrigerant pressure. The function logic is shown in Figure 7.3-37.

CCWS Actuation from Safety Injection Signal

Upon receipt of a safety injection signal, the four CCWS trains are started, supplying all SIS pump coolers and the four LHSI heat exchangers. The non-safety-related users outside of the RB are also isolated.

The system response optimizes the CCWS to cool the SIS pumps and LHSI heat exchangers. The following CCWS actuations are automatically initiated:

- Start CCWS pumps (KAA10/20/30/40 AP001), if not previously running.
- Open LHSI HX isolation valves (KAA12/22/32/42 AA005).
- Open LHSI pump seal cooler isolation valves (KAA22/32 AA013).
- Close isolation valves for non-safety related users outside of RB (KAB50 AA001/004/006 & KAB80 AA015/016/019).

Simultaneous operation of LHSI heat exchanger isolation valves (opening) and non-safety-related user isolation valves (closing) maintains pump operation in a safe range.

A safety injection signal initiates a concurrent containment isolation Stage 1 signal.

CCWS Operation from Containment Isolation Stage 1

Upon receipt of a containment isolation stage 1 signal, CONT HVAC and NI DVS users in the RB are isolated via closure of KAB40 AA001/006/012.

This system response isolates these users, confirms the containment isolation function is met, and allows a maximum cooling flow rate through the LHSI heat exchanger in the event of a coincident safety injection signal.

CCWS Operation from Containment Isolation Stage 2

Upon receipt of a containment isolation stage 2 signal, the RCP and CVCS loads inside the RB are isolated (not including the RCP thermal barriers) via closure of KAB60/70 AA013/018/019.

CCWS Response to a LOOP

In case of LOOP, operating CCWS trains are de-energized. Previously operating CCWS trains return to operation according to the EDG load sequencing and standby trains remain idle, unless other start signals are received during EDG load sequencing.

CCWS Switchover Valve Interlock

Train separation of redundant CCWS divisions confirms that a fault affects no more than one train via a switchover valve interlock. To prohibit more than one train from being connected to a common header, the following groupings of valves cannot be simultaneously opened:

- Common 1.a – KAA10AA032/033 with KAA20AA032/033.
- Common 2.a – KAA30AA032/033 with KAA40AA032/033.
- Common 1.b – KAA10AA006/010 and KAA20AA006/010.
- Common 2.b – KAA30AA006/010 and KAA40AA006/010.

The functional logic is shown on Figure 7.6-1.

~~*Thermal Barrier Isolation*~~

~~A fault of an RCP thermal barrier is recognized by the following indications:~~

- ~~A high flow above a threshold value measured with a flow element in the CCWS piping on the return from each RCP thermal barrier.~~
- ~~A high pressure above a threshold value measured with a pressure sensor in the RCS piping on the return from each RCP thermal barrier.~~

~~Isolation valves at inlet (JEB10/20/30/40 AA021) and outlet (JEB10/20/30/40 AA003) of each RCP thermal barrier (as shown in Figure 5.1-4) are used to automatically isolate the faulted thermal barrier from the CCWS. High radiation in the CCWS does not initiate automatic isolation of CCWS cooling to the RCP thermal barriers. Isolation of faulted RCP thermal barrier only affects that RCP; it does not affect the CCWS cooling of the other three RCP thermal barriers or thermal barrier cross tie.~~

CCWS RCP Thermal Barrier Containment Isolation Valve Interlock

Either the common 1.b or 2.b headers can provide cooling to the RCP thermal barriers. To maintain strict train separation of the redundant CCWS division supplying either common header to confirm that a fault affects no more than one train, the CIVs (KAB30 AA049/050/051/052/053/054/055/056) are interlocked. One of the two common 1.b supply valves (KAB30 AA049/050) and one of the two common 1.b return valves (KAB30 AA051/052) must be closed prior to opening the CIVs from the common 2.b header (KAB30 AA053/054/055/056), and vice versa. The functional logic is shown on Figure 7.6-2.

To maintain cooling to the RCP thermal barriers an interlock function is required to open the CIVs on the common header removed from service (common 1.b or 2.b) when a CIV on the common header in service (common 2.b or 1b, respectively) is closed. The functional logic is shown on Figure 7.6-12.

9.2.2.6.1.2 CCWS Manual I&C Safety-Related Functions

CCWS Manual Control

Safety-related manual controls are provided for the operators in the MCR as a backup to the SR system automation. Manual control capabilities are provided in the MCR for the following CCWS components:

- CCWS pump (30KAA10/20/30/40 AP001).
- CCWS switchover valves (30KAA10/20/30/40 AA006/010/032/033).
- CCWS heat exchanger bypass valve (KAA10/20/30/40 AA112).
- Non-safety-related branch Isolation valves (KAB50 AA001/004/006, KAB80 AA015/016/019).
- CIVs.

CCWS Common 1.a (2.a) Manual Supply

When the common 1.b (2.b) header supply is automatically transferred to the common header associated CCWS train via the automatic switchover sequence, the common 1.a (2.a) header is also isolated and no automation is foreseen to switchover the common

- When the surge tank water level lowers to the MIN1 level, the DWDS supply isolation valve (KAA10/20/30/40 AA027) is automatically opened.
- When the surge tank water level reaches the MAX1 level, the DWDS supply isolation valve is automatically closed.

RCP Thermal Barrier Cooling Transfer

Either the common 1.b or 2.b headers can provide cooling to the RCP thermal barriers. Because of the valve interlock associated with the supply of cooling to these loads and the short duration desired to have cooling flow isolated, a group command is provided. The RCP thermal barrier cooling transfer consists of closing the open group of CIVs (KAB30 AA049/050/051/052, common 1.b or KAB30 AA053/054/055/056, common 2.b) and as soon as one of the two supply valves on the initial header and one of the two return valves on the initial header indicate closure, the other group of CIVs (KAB30 AA049/050/051/052, common 1.b or KAB30 AA053/054/055/056, common 2.b) are opened.

In case a CIV fails to open on the final header, another transfer is automatically performed back to the initial configuration.

In the event that one CCWS train is inoperable, RCP thermal barrier cooling is aligned to the CCWS common header that is supported by two operable CCWS trains within 72 hours per Chapter 16, Technical Specification 3.7.7.

RCP Thermal Barrier Isolation

A fault of an RCP thermal barrier is recognized by the following indications:

- A high flow above a threshold value measured with a flow element in the CCWS piping on the return from each RCP thermal barrier.
- A high pressure above a threshold value measured with a pressure sensor in the RCS piping on the return from each RCP thermal barrier.

Isolation valves at inlet (JEB10/20/30/40 AA021) and outlet (JEB10/20/30/40 AA003) of each RCP thermal barrier (as shown in Figure 5.1-4) are used to automatically isolate the faulted thermal barrier from the CCWS. High radiation in the CCWS does not initiate automatic isolation of CCWS cooling to the RCP thermal barriers. Isolation of faulted RCP thermal barrier only affects that RCP; it does not affect the CCWS cooling of the other three RCP thermal barriers or thermal barrier cross tie.

CCWS Temperature Control

Normally, the CCWS heat exchanger bypass control valve (KAA10/20/30/40 AA112) is manually positioned in order to maintain a CCWS normal temperature greater than 59°F and less than 100.4°F. This is a remote manual operation from the MCR. An

CREF (Iodine Filtration) Train Subsystem

The CREF (iodine filtration) train subsystem is illustrated in Figure 9.4.1-1.

The train 1 outside air inlet duct and train 1 CREF (iodine filtration) train is located in Safeguard Building 2. The train 4 outside air inlet duct and train 4 CREF (iodine filtration) train is located in Safeguard Building 3. Each CREF (iodine filtration) train pulls air from its respective outside air inlet. The outside inlet air for each CREF is ducted to allow the CREF (iodine filtration) train to operate in the filtered or the unfiltered (bypass) alignment.

In the CREF filtered alignment, a maximum of 1000 cfm of outside air mixes with 3000 cfm of CRE recirculated air and is pulled through the CREF (iodine filtration) train by the CREF booster fan and delivers this air to the common recirculation plenum. In the filtered alignment, the filter bypass duct has two motor-operated bypass dampers in series. In the filtered alignment both of these dampers close to provide redundancy and single-failure protection to prevent the outside air from bypassing the CREF (iodine filtration) trains.

In the CREF unfiltered (bypass) alignment, the CREF filtration unit inlet, outlet and CRE recirculation dampers are all closed and both bypass dampers are open. The outside unfiltered air bypasses the CREF iodine filtration unit. In the unfiltered (bypass) alignment, the outside air flows through a prefilter and a preheater that is temperature controlled. The outside air then flows through ducting and is pulled into the common recirculation plenum. In this unfiltered (bypass) alignment, the CREF booster fan does not operate and outside air is pulled into the common recirculation plenum by the CRACS air handling units.

Air Conditioning and Recirculation Air Handling Subsystem

The air conditioning and recirculation air handling subsystem is illustrated in Figure 9.4.1-2—Control Room Air Conditioning and Recirculation Air Handling Subsystem.

There are four recirculation air handling units located in Safeguard Buildings 2 and 3 (two trains in each building). Recirculated and fresh air is processed through these air handling units and supplied to a common supply air plenum. Each train includes an isolation damper, a volume control manual damper, a cooling coil, a moisture separator, fan suction and discharge silencers, a supply air fan, a HEPA filter, and a non-return damper. The cooling coil is supplied with chilled water from the safety chilled water system (SCWS).

During normal and emergency operation, each CRACS cooling unit provides 50 percent of the cooling for the rooms within the CRE. Each CRACS air handling unit is designed for 50 percent cooling of the normal and emergency cooling load to allow

Fans

The supply and exhaust fans are centrifugal or vane axial type with electric motor drivers that are direct drive. Fan performance is rated in accordance with ANSI/AMCA 210~~-99~~ (Reference 4), ~~ANSI/~~AMCA 211~~-1987~~ (Reference 5) and ANSI/AMCA 300~~-1985~~ (Reference 6).

Isolation dampers

Manual dampers are adjusted during initial plant startup testing to establish accurate air flow balance between the rooms. The motor-operated isolation dampers will fail as-is~~in position~~ in case of power loss. Backdraft dampers prevent air flow to non-operating air supply and exhaust trains. The performance and testing requirements of the dampers are per ASME AG-1 (Reference 1).

Fire Dampers

Fire dampers are installed in fire barrier walls or floors. Fire damper design meets the requirements of ~~UL 555~~ NFPA 80 (Reference 7) and NFPA 90A (Reference 18) and the damper fire rating is commensurate with the fire rating of the barrier penetrated. Fire dampers are equipped with fusible links for automatic closure when the temperature reaches a predetermined setpoint.

Cooling Coils and Moisture Separator

The cooling coils are of the finned tube, coil type and are connected to the safety chilled water system (SCWS). The cooling coils have a total cooling capacity of 470,000 Btu/hr and are designed in accordance with ASME AG-1 (Reference 1). The moisture separator collects condensate which is directed to the drain system.

9.4.1.2.3 System Operation

Normal Plant Operation

During normal plant operation, fresh air is admitted via air intake trains 1 and 4. The fresh air passes through the unfiltered bypass duct and bypass dampers. The fresh air is then mixed with the recirculated air from the CRE area, and the mixed air passes through a prefilter and electrical heater. Two sets of temperature sensors are located downstream of the electrical heater. One temperature sensor turns on the heater when the air inlet temperature drops below 37°F; the other temperature sensor turns off the heater when the air inlet temperature reaches 50°F.

The fresh and recirculated air is admitted through two of four air handling units which provide heating and cooling of the supply air. The conditioned air is then distributed through a ductwork distribution network to the CRE area. The room air conditioning

train during any design basis accident will not result in a loss of iodine filtration capability because two CREF (iodine filtration) trains are provided.

Loss of Coolant Accident

Upon receipt of a containment isolation signal, the following functions are initiated automatically:

- Opens Control Room Emergency Filtration (CREF) iodine filtration trains isolation dampers.
- Closes CREF iodine filtration trains bypass dampers.
- Opens Control Room Envelope (CRE) recirculation dampers to provide clean air and positive pressurization for the rooms within the CRE.

Loss of Offsite Power

During loss of offsite power (LOOP), the air intake and air conditioning and recirculation air handling electrical components located inside SB division two receive power for one train from the emergency diesel generators (EDG) of division two, and for the other train from the EDGs of division one. The electrical components located inside the SB division three receive power on one train from the EDGs of division three, and for the other train from the EDGs of division four.

During LOOP, the CREF (iodine filtration) train electrical components located inside the SB division two receive power from the EDGs of division one. The electrical components located inside the SB division three receive power from the EDGs of division four.

Station Blackout

- In the event of station blackout (SBO), the electrical components, which receive power from the EDGs of divisions one and two, are backed-up by alternate AC (AAC) power from the SBO diesel generators (SBODG) of ~~division~~ train one. The electrical components, which receive power from the EDGs of divisions three and four, are backed up by the AAC power from the SBODG~~s~~ of ~~division~~ train two~~four~~.
- In the event of a simultaneous SBO and site radiological event, the CRE area is isolated and CRACS is maintained in a full recirculation mode through the CREF (iodine filtration) train until site power is restored or EDGs are started. Power restoration is assumed to occur within eight hours following the occurrence of a SBO event.

Loss of Ultimate Heat Sink

The conditioned air supply is cooled by chilled water provided by the SCWS. Two water-cooled chillers are located in SB divisions two and three, and two air-cooled

Fuel Handling Accident in the Containment Building

In the event of a fuel handling accident in the Containment Building, to preclude uncontrolled migration of contamination, the FB areas in front of the emergency airlock and in front of the equipment hatch are isolated by closing the air exhaust and supply dampers dedicated to these areas.

Prior to opening the emergency airlock during an outage, the air exhaust in front of the emergency airlock is isolated by closing the dampers dedicated to this area.

Prior to opening the equipment hatch during an outage, the air supply and exhaust for the equipment area in front of the hatch are isolated by closing the dampers dedicated to this area.

Loss of Coolant Accident (LOCA)

Upon receipt of a containment isolation signal, the following functions are initiated automatically:

- Closes FBVS exhaust air isolation dampers to NABVS.
- Closes FBVS supply air isolation dampers from NABVS.
- Opens FBVS exhaust air isolation dampers to exhaust air from the entire Fuel Building to the SBVS.
- Opens isolation dampers for the SBVS Accident Exhaust Iodine Filtration Trains.
- Starts SBVS iodine filtration train fans to pull air through SBVS Accident Exhaust Iodine Filtration Trains and to direct exhaust air to the vent stack. The SBVS maintains negative pressure in the Fuel Building.

Loss of Offsite Power (LOOP)

~~Upon loss of offsite power, all motorized dampers will fail as is, limiting pathways for potentially contaminated air to leak out to the environment.~~

The following equipment will remain operational during LOOP:

- Electric heaters in the extra borating pump rooms and pipe chase.
- Recirculation cooling units in the fuel pool cooling system pump rooms, and extra borating system pump rooms.
- Dampers for isolating the fuel pool room and FB.

The power for the equipment listed above is supplied from the corresponding emergency diesel generators.

The outside air is provided through intake mesh grills and louver dampers. The outside air intake openings are equipped with electrically heated and weather protected grills to prevent ice formation and ingress of insects and debris. The intakes are designed to provide adequate outside air to meet the distribution requirements of supply air under design conditions of the plant.

Deleted - humidifier,

The air intake plenum supplies air through three filtration trains. Each train consists of a preheater, prefilter, cooling coil, heater, silencer, and air dampers. Four supply air fans take suction from the supply fan inlet plenum and supply air to the outlet air shaft for further distribution to the supply shafts of different buildings.

The design supply air flow to serve the NAB, FB, annulus ventilation system, and Containment Building would require all three trains to be in operation. However, during normal operation, a reduced air flow rate can be used that requires only one supply train to be in operation.

Nuclear Auxiliary Building Air Supply Subsystem

This subsystem supplies air to the NAB to maintain ambient conditions within the prescribed limits for equipment operation and personnel access. See Figure 9.4.3-2—Nuclear Auxiliary Building Air Supply and Exhaust Subsystem.

The conditioned air is supplied to all levels of the building through air shaft cells and a duct distribution network. The flow rate to each room is calculated based on the room volume and equipment heat loads to maintain ambient conditions. The normal operation of the system is to maintain a negative pressure in the building with respect to the outside atmosphere to prevent leakage of potentially contaminated air to the environment. The air flow paths within the NAB are designed so that if radiation is detected, migration of contaminated air from areas of potentially high radioactivity to areas of potentially low radioactivity is limited.

The recirculation cooling units are provided for the rooms with high heat loads. Cooling coil units with fans provide recycled cooled air to the rooms where vapor compressors, electrical switchgear, and transformers are located.

Exhaust Air Subsystem

This subsystem processes exhaust air through filtration trains and charcoal filtration trains to limit airborne radioactivity released through the vent stack. See Figure 9.4.3-3—Nuclear Auxiliary Building Exhaust Filtration Trains Subsystem.

The system processes air exhaust from the following areas:

- FB Cell 5 exhaust (refer to Section 9.4.2).
- FB Cell 4 exhaust (refer to Section 9.4.2).

Ductwork and Accessories

The supply and exhaust air ducts are constructed of galvanized sheet steel and are structurally designed for fan shutoff pressures. The ductwork meets the design, testing and construction requirements per ASME AG-1 (Reference 1).

Heaters

Deleted paragraph.

Supply air trains have hot water heaters. The heater design is based on the minimum outside air design temperature and supply air temperature requirements. The coils are constructed and tested in accordance with ASME AG-1 (Reference 1). Electric heaters are located upstream of iodine filters to prevent excessive moisture accumulation in the charcoal beds.

Prefilters

The prefilters are located upstream of HEPA filters and collect large particles to increase the useful life of the ~~high efficiency~~HEPA filters. The prefilters will meet the requirements of ANSI/ASHRAE Standard 52.2~~-1999~~ (Reference 2).

HEPA Filters

HEPA filters are constructed, qualified and tested in accordance with ASME AG-1 (Reference 1). The periodic in-place testing of HEPA filters to determine the leak-tightness is performed per ANSI/ASME N510~~-1989~~ (Reference 3).

Adsorbers

Carbon filters are used to remove radioactive iodine from the exhaust air. The efficiency for removal of methyl iodine is based on the decontamination efficiency assigned during the laboratory tests. The periodic in-place testing of the adsorbers to determine the leak-tightness is performed per ANSI/ASME N510 (Reference 3). The activated carbon total bed depth requirement will be 2 inches with a maximum assigned activated carbon decontamination efficiency of 95 percent.

Post Filters

The post filter is located downstream of the carbon adsorber. During operation of the carbon filtration exhaust, the air flow rate will be low through the carbon adsorber to prevent spread of the carbon dust. However, the post filter ensures that carbon dust or carbon fines are removed prior to the air being distributed further. The post filter meets the requirements of ASME AG-1 (Reference 1), and has an average atmospheric dust efficiency of 95% in accordance with ANSI/ASHRAE Standard 52.2 (Reference 2). The post filter is equipped with differential pressure measurement which indicates the degree of particulate loading and the need for filter change.

within prescribed limits for operation of equipment and the safety and comfort of personnel.

The SBVS air supply and exhaust flows are designed to prevent the spread of airborne contamination and to maintain a negative pressure in the hot mechanical areas of the SBs with respect to the outside environment.

The SBVS has two separate modes of exhaust:

- Operational Air Exhaust Mode–The exhaust air (normal exhaust) from all four divisions of the SBs (hot mechanical areas) connects to a single concrete duct in the annulus, which then runs via the FB and connects to the exhaust duct of the NABVS. The exhaust duct of each SBVS train ~~division~~ is equipped with two isolation dampers and one volume control damper. The exhaust air is processed by the NABVS through a filtration train prior to release through the vent~~plant~~ stack (refer to Section 9.4.3).

- Accident Air Exhaust Mode–If airborne contamination is detected in any of the four hot mechanical areas of the SBs or there is a containment isolation signal, the SBVS will automatically direct the exhaust air (accident exhaust) via four separate exhaust air ducts, ~~and~~ each with two parallel isolation dampers, to one common concrete duct in the annulus. This exhaust duct connects to two accident iodine exhaust filtration trains located in the FB. The exhaust air is processed through one of two redundant and independent iodine filtration trains prior to release through the vent ~~plant~~ stack. Each iodine filtration train includes inlet and outlet dampers, moisture separator, two stage electric heater, prefilter, ~~inlet and outlet~~ high efficiency particulate air (HEPA) filter~~s~~, carbon adsorber, post filter, exhaust fan, and backdraft damper. The fans direct the exhaust air to the vent~~plant~~ stack.

In case of a fuel handling accident in the FB, the accident exhaust air from ~~these buildings~~the FB is directed and filtered through the SBVS iodine exhaust filtration trains located in the FB, and released through the vent ~~plant~~ stack.

In case of containment isolation signal, the SBVS maintains a negative pressure and filters all areas of the FB and the hot mechanical area of the SB in addition to performing the SBVS accident air exhaust filtration function.

The supply and exhaust duct network of the hot mechanical area in the SBs is equipped with isolation dampers to isolate the following areas from the other rooms:

- Rooms where safety injection and residual heat removal system components in divisions one through~~and~~ four are installed.

- Rooms where severe accident heat removal system components in division four are installed.

- Personnel air lock area in division two.

Moisture Separator

The moisture separator meets the requirements of RG 1.52 (Reference 10), ANSI/ ASME N509 (Reference 9), and ASME AG-1 (Reference 2). The moisture separator is located upstream of the filter air heater and the prefilter to protect the HEPA filter and carbon adsorber from potentially high humidity level by removing the entrained water droplets from the inlet air stream. The moisture separator design shall be qualified by testing in accordance with the procedure described in ANSI/ASME N509. ~~The moisture separator is a combination of moisture separator and prefilter. The moisture separator must meet the requirements of RG 1.52 (Reference 10), ASME N509 (Reference 9), and ASME AG-1 (Reference 2). The moisture separator is located upstream of the filter air heater and the HEPA prefilter. The moisture separator shall be a design that has been qualified by testing in accordance with the procedures described in Reference 9.~~

Filter Air Heaters

Two stage electric heaters are located upstream of HEPA and iodine filtration units to prevent excessive moisture accumulation in the charcoal filter beds. At the start of an accident, full power of two stage electric heater is switched on when the fans start and filter bank isolation dampers open. As the negative pressure is drawn in the FB and SB, and when the temperature downstream of heater increases to 158°F, one step of heater power is switched off automatically. As the temperature downstream of heater reaches 176°F, second step of the heater is also switched off automatically. The heaters meet the requirements of ASME AG-1 (Reference 2).

Prefilters

The prefilters are located upstream of the HEPA filters and collect large particles to increase the useful life of the ~~high efficiency~~ HEPA filters. The prefilters meet the requirements of ANSI/ASHRAE Standard 52.2 ~~1999~~ (Reference 3).

HEPA Filters

HEPA filters are constructed, qualified and tested in accordance with ASME AG-1 (Reference 2). The periodic inplace testing of HEPA filters to determine the leak tightness is performed per ANSI/ASME N510 ~~1989~~ (Reference 4).

Adsorbers

Carbon adsorbers are used to remove radioactive iodine from the exhaust air. The efficiency for removal of methyl iodine is based on the decontamination efficiency assigned during the laboratory tests. The periodic inplace testing of adsorbers to determine the leak-tightness is performed per Reference 4.

- Recirculation cooling units in the SB divisions one and four, where the EFW valves are located.

Loss of Ultimate Heat Sink

During loss of ultimate heat sink (LUHS), the air flow of the recirculation cooling units is cooled by the chilled water provided by the SCWS. Two water-cooled chillers are located in SB divisions two and three, and two air-cooled chillers are located in SB divisions one and four. In case of LUHS, the water-cooled chillers are not available. With the safety chilled water divisions 1/2 or divisions ~~and~~ 3/4 interconnect, the safety chilled water is then supplied by air-cooled chillers which provide the cooling function for the recirculation cooling units located in divisions one, two, three and four.

Loss of Coolant Accident

Upon receipt of a containment isolation signal, the following functions are initiated automatically:

- Closes SBVS supply air isolation dampers from SBVSE.
- Closes SBVS exhaust air isolation dampers to NABVS.
- Opens SBVS exhaust air isolation dampers to exhaust air from the hot mechanical areas of SB and the FB to the SBVS Accident Exhaust Iodine Filtration Trains (located in the FB).
- Opens isolation dampers for the SBVS Accident Exhaust Iodine Filtration Trains.
- Starts SBVS iodine filtration train fans to pull air through SBVS Accident Exhaust Iodine Filtration Trains and to direct exhaust air to the vent stack.

In the event of a LOCA, the containment isolation signal initiates isolation of the FB from NABVS supply and exhaust duct to limit leakage into the FB. The SBVS maintains a negative pressure in the FB and exhaust air from the FB is directed to the SBVS iodine filtration trains (refer to Section 9.4.2).

Iodine Presence in the SB Rooms

In the event of a failed fuel element and residual heat removal pump seal leakage, high iodine is expected to be present in only one of the four SB divisions at a time, and it is necessary to purify the air in this division for personnel access. The air supply and exhaust flow for the affected division is increased to purge the possibly contaminated areas, while air supply and exhaust for the other three divisions is decreased. This is achieved by ~~opening or closing the isolation dampers and~~ partially opening the exhaust volume control dampers and by partially closing the exhaust volume control dampers of the other three divisions in order to maintain an acceptable total exhaust

- The cooling supply units are designed to provide cooling as required to prevent the SBVSE room temperatures from exceeding their maximum design temperature.

- Winter heating loads will be calculated with the plant operating in an outage alignment configuration. Winter heat loads will be calculated with a minimum outside air design temperature 0 percent exceedance value, using U.S. EPR Site Design Envelope Temperature (See Table 2.1-1).

- The SBVSE supply air duct heaters are designed to operate as required when the supply air temperature is less than the minimum set point value.

With outside air ambient design temperature conditions of -40°F to 115°F, the SBVSE maintains the following temperature and humidity ranges for the areas serviced.

Room	Temperature	Humidity
Rest Rooms, changing rooms	65°F - 78°F	10 - 60%
RSS	65°F - 78°F	10 - 60%
Switchgear Rooms	59°F - 104°F	10 - 60%
Cable Floor	41°F - 95°F	10 - 60%
I&C Equipment Room	68°F - 82°F	10 - 60%
Battery Rooms	65°F - 77°F	10 - 60%
HVAC Rooms	50°F - 95°F	10 - 80%
Non-controlled (~~C~~cold) Mechanical Areas, Emergency Feedwater Pump Rooms, and Component Cooling Water Pump Rooms	41°F - 104°F	10 - 60%
Corridors	50°F - 104°F	10 - 60%

The SBVSE performs the following safety-related system functions:

- Maintains acceptable ambient conditions for the safety-related components in the electrical and instrumentation and controls (I&C) rooms in the SB during accident conditions, taking into account internal and external heat loads.

- Maintains acceptable ambient conditions inside the emergency feed water system (EFWS) pumps and component cooling water system (CCWS) component rooms of the SB during accident conditions, taking into account internal and external heat loads.

Additional electric heaters installed in supply air ducts are used to maintain the minimum temperatures in battery rooms and toilet rooms.

For each train~~division~~, the SBVSE consists of:

- A single air intake equipped with a damper and grilles. The SBVSE air intakes in SB divisions 2 and 3 are common for the main control room (MCR) air conditioning system (CRACS) (refer to Section 9.4.1) and smoke confinement system (SCS) of the same division (refer to Section 9.4.13).
- A safety-related air conditioning train. Mixing is done with control dampers, filtration with filters, heating with electric ~~air~~ heater, and cooling with air cooling coil,. The train also has the associated exhaust air train, with exhaust fan and control damper.
- A connection with a non-safety-related air conditioning train. Mixing is done with control dampers, filtration with filters, heating with electric ~~air~~ heater, cooling with air cooling coil, and ventilation with supply air fan. The train also has the associated exhaust air train, with exhaust fan and control damper.
- Cross-connected ducts between divisions 1 and 2 and divisions 4 and 3 for the HVAC supply and exhaust with the non-safety-related maintenance trains for use when one SBVSE safety-related train of division 2 or 3 is unavailable. Manual isolation dampers equipped with "opened" and "closed" limit switches are installed in the cross-connected ducts (i.e., supply and exhaust ducts of division 1 and 2 and division 3 and 4).
- Connections providing air to the mechanical controlled area (interface with SBVS).
- A single ductwork providing air to the electrical rooms and mechanical non-controlled rooms.
- Two independent exhaust ductworks:
  - The first exhaust ductwork is used for the rooms in the non-controlled area of the SB, except for rooms served by the second exhaust ductwork. It is connected to one of the two recirculation-exhaust fans. One of the fans is a safety-related fan and is located in the same division. The other is a non-safety-related fan for maintenance operation, which is common for the two combined divisions 1 and 2 (located in division 1) and the two combined divisions 3 and 4 (located in division 4). The exhaust air of transformers and inverters is directly exhausted through exhaust hoods above the equipment.
  - The second exhaust ductwork is used for the rooms which could accumulate specific gas (hydrogen in the battery rooms and refrigerant gas in the rooms of the SCWS) and for the non-controlled mechanical area. The air is directly exhausted outside using one of two exhaust fans (one safety-related fan, or one non-safety-related maintenance fan). For the battery rooms, a bypass

- Air cooling coil of finned tube coil type has a total cooling capacity of 1,134,900 Btu/hr, supplied with chilled water by the SCWS of the same division.
- Droplet separator, connected to the nuclear island drain and vent system (NIDVS).
- Silencer on fan suction side, splitter type.
- Supply air fan, free wheel radial type, direct driven, with a design air flow of 29,500 scfm.

Deleted paragraph.

- Non-return damper.
- Silencer on fan discharge side, splitter type.

Recirculation-Exhaust Air – Safety-Related Train

The recirculation and exhaust air trains are located in divisions 1 and 4 at elevation +39 ft and in divisions 2 and 3 at elevation +69 ft.

Each train includes:

- Isolation dampers, manually operated.
- Recirculation and exhaust air fan, radial type, direct driven, with a design air flow of 29,500 scfm.
- Control damper with electrical actuator.
- Non-return damper.
- Isolation damper, manually operated.
- Dampers.
- Weather protection grilles.

Exhaust Air for Battery-Safety Chilled Water Room and Non-controlled Mechanical Area – Safety-Related Train

The exhaust air trains are located in divisions 1 and 4 at elevation +39 ft and in divisions 2 and 3 at elevation +69 ft.

Each train includes:

- Isolation damper, manually operated.
- Exhaust air fan, radial type, direct driven.
- Non-return damper.

- Isolation damper with electrical actuator.

Supply Air System – Maintenance Train

The maintenance train is non-safety-related. The supply air units are located in divisions 1 and 4 at elevation +39 ft. The components are installed in a sheet metal structure.

Each air conditioning train includes:

- Insect protection screen.
- Isolation damper, manually operated.
- Set of control dampers with electrical actuator.
- Prefilter.
- Roughing filter.
- Electric heater, with tubular elements, comprised of four heating stages.
- Air cooling coil of finned tube coil type, has a total cooling capacity of 1,134,900 Btu/hr supplied with chilled water by the operational chilled water system (OCWS).
- Droplet separator, connected to the NIDVS.
- Silencer on fan suction side, splitter type.
- Supply air fan, free wheel radial type, direct driven, with a design air flow of 29,500 scfm.

Deleted paragraph.

- Non-return damper.
- Silencer on fan discharge side, splitter type.

Recirculation-Exhaust Air – Maintenance Train

The maintenance train is non-safety related. The recirculation-exhaust air trains are located in divisions 1 and 4 at elevation +39 ft.

Each train includes:

- Isolation dampers, manually operated.
- Recirculation and exhaust air fan, radial type, direct driven, with a design air flow of 29,500 scfm.
- Control damper with electrical actuator.

- Non-return damper.
- Isolation damper, manually operated.

9.4.6.2.3 System Operation

Normal Plant Operation

The SBVSE operates during normal plant operation and during outage conditions. The HVAC for each division (1 to 4) is provided by an air supply train and associated exhaust train (with the same safety classification). The normal operation for each division follows:

- The safety-related train is in service to provide filtration, heating, and cooling. Outside makeup air is supplied to each train of the SBVSE through a separate air intake. This outside air mixes with the recirculated air upstream of the supply air filters. The amount of outside air admitted depends on the outside air temperature and is automatically adjusted by control dampers. If required, air heating is performed by the electric ~~air~~ heater. Air cooling is performed by the air cooling coil. The supply air fan supplies the air to the rooms of the SB division.
- The maintenance train (non-safety-related) for supply air and exhaust air is shut down.
- Air is supplied to the non-contaminable rooms of the SB plus the hot (controlled) mechanical area, which is exhausted by the SBVS.
- Air is exhausted from all rooms, except the controlled area exhausted by the SBVS.
- Air is released from the rooms representing the risk of accumulation of specific gas (i.e., hydrogen in battery rooms and refrigerant gas in SCWS room) and the rooms of the ~~cold (i.e., non-controlled)~~ mechanical area to the outside by a dedicated exhaust fan.
- Exhaust air is released from the toilet rooms of division 1 and 4 to the outside, also by a dedicated exhaust fan.
- The exhaust air of the remaining rooms is collected and directed to the recirculation-exhaust fan where a portion of the air can be recirculated or directly discharged to the outside. The amount of air to be recirculated depends on the outside air temperature and is automatically adjusted by the control damper.
- Ventilation tasks of the RSS, located in division 3, are provided by the SBVSE of the neighboring division 2.
- The recirculation cooling units are in automatic operation, and the fans are operated in ON-OFF mode depending on the room temperature.
- Electric heaters in supply air ducts, for example for battery rooms, are in automatic operation and are operated in ON-OFF mode depending on the room temperature.

Failure of a SBVSE component will not adversely affect the operation of the interfacing systems SCWS or OCWS.

If the SBVSE in one division fails, switchover from the safety-related train to the maintenance train of either division 1 or 2 or division 3 or 4 is possible. Therefore, ventilation of electrical and I&C equipment in all divisions is provided even in case of failure of one of the four divisions.

Additionally, the SCWS has the same configuration as the SBVSE. If the SCWS in one division fails, switchover from the safety-related train to the maintenance train in either division 1 and 2 or division 3 and 4 is possible.

If a failure of a safety-related train of the SB is postulated during maintenance of an SB HVAC train, two SB trains remain available.

Loss of Offsite Power (LOOP)

In case of LOOP, fans and actuators of each safety-related train of the SBVSE (division 1 to division 4) are backed up by the corresponding emergency diesel generator.

Loss of Ultimate Heat Sink (LUHS)

For the SBVSE, the chilled water to the safety trains is provided by the SCWS, with the following key features:

- Two water-cooled chillers, cooled by the CCWS, in divisions 2 and 3.
- Two air-cooled chillers at elevation +39 ft in divisions 1 and 4.

In case of loss of ultimate heat sink (LUHS), the SCWS air-cooled chillers will continue to provide the cooling function of the SBVSE of the two divisions 1, 2, 3, and 4.

9.4.6.3 Safety Evaluation

The safety-related portion of the SBVSE is located in the associated SB. The SB is a Seismic Category I structure that is designed to withstand the effects of earthquakes, tornadoes, hurricanes, floods, external missiles, and other appropriate natural phenomena. Sections 3.3, 3.4, 3.5, 3.7, and 3.8 provide the bases for the adequacy of the structural design of this building.

The safety-related portion of the SBVSE is designed to remain functional after a safe shutdown earthquake (SSE). Sections 3.7 and 3.9 provide the design loading conditions. Sections 3.5, 3.6 and 9.5.1 provide the hazards analyses to demonstrate that a safe shutdown, as outlined in Section 7.4, can be achieved and maintained.

9.4.9 Emergency Power Generating Building Ventilation System

The emergency power generating building ventilation system (EPGBVS) maintains acceptable ambient conditions and air renewals of the diesel hall, electrical room, and main tank room of each of the four divisions of the Emergency Power Generating Buildings (EPGB). Each division has its own independent heating, ventilation and air conditioning (HVAC) system which is not connected to other divisions. Two divisions are located in each of the two EPGBs.

9.4.9.1 Design Bases

The EPGBVS consists of safety-related and non-safety-related air supply and exhaust systems. The safety-related portion is designed to Seismic Category I requirements, and the non-safety-related portion is designed to Seismic Category II requirements. The EPGBVS performs the following safety-related system function and complies with the general design criteria (GDC) indicated below:

- The EPGBVS maintains acceptable temperatures and air renewals in each of the four divisions to support the operation of the emergency diesel generators (EDG) and electrical control panels. The EDGs are required to provide onsite emergency power for the safety-related equipment to achieve and maintain the plant in a safe shutdown condition following a design basis accident, including loss of offsite power (LOOP).

- In accordance with GDC 2, the EPGBVS components are located inside the EPGBs, which are designed to withstand the effects of natural phenomena, such as earthquakes, tornados, hurricanes, floods and external missiles.

- In accordance with GDC 4, the EPGBVS components remain functional and continue to perform their intended safety function after anticipated operational occurrences and design basis accidents, such as fire, internal missiles, or pipe breaks.

- In accordance with GDC 5, the safety-related components and systems of the EPGBVS are not shared with other nuclear power units.

- In accordance with GDC 17, the U.S. EPR contains an onsite and offsite electric power system that supports the functioning of structures, systems, and components important to safety in the event of postulated accidents and anticipated operational occurrences. The EPGBVS maintains a minimum clearance of 20 feet from the bottom of fresh air intakes to grade elevation, and electrical cabinets are provided with suitable seals or gaskets, These features maintain proper functioning of the essential electric power system by meeting the guidelines of NUREG-CR/0660 (Reference 1), as related to the accumulation of dust and particulate material.

  The essential onsite electrical power systems meet the guidance of NUREG-CR/0660 for protection of essential electrical components (such as contactors, relays, circuit breakers) from failure due to the accumulation of dust and particulate

materials. This is accomplished by the use of filters and supply air units in the EPGBVS.

Air conditioning and heating loads for the EDG rooms are calculated using methodology identified in ASHRAE Handbook (Reference 8).

- Summer cooling loads will be calculated with a maximum outside air design temperature 0 percent exceedance value, using U.S. EPR Site Design Envelope Temperature (See Table 2.1-1). The analysis will be completed for both a normal and accident plant alignment configuration with EDG in operation.

- The cooling supply units are designed to provide outside air for cooling as required to prevent the EDG room temperatures from exceeding their maximum design temperature.

- Winter heating loads will be calculated with the plant operating in an outage alignment configuration, without diesel operation. Winter heat loads will be calculated with a minimum outside air design temperature 0 percent exceedance value, using U.S. EPR Site Design Envelope Temperature (See Table 2.1-1).

Though the EDGs are in standby mode during normal plant operation, the EPGBVS is available in any plant operating condition. With outside air ambient design temperature conditions of -40°F to 115°F, the EPGBVS is designed to meet the following safety-related functional criteria:

- Maintains the diesel hall temperature between 59°F and 140°F.

- Maintains the electrical room temperature between 40°F and 113°F with 35 to 70 percent relative humidity.

- Maintains the main tank room temperature between 59°F and 120°F.

The EPGBVS performs the following non-safety system functions:

- Provide outside air and cooling to the diesel hall when the EDGs are not in operation, or safety-related supply and exhaust fans are not required to operate.

- Provide outside air and cooling to the electrical room.

9.4.9.2 System Description

9.4.9.2.1 General Description

The EPGBVS ventilates the diesel generators using outside air as the cooling medium. Air is supplied into the building to slightly pressurize the building, and is then vented from the building through exhaust air louver openings.

The EPGBVS includes ventilation of diesel divisions 1 through 4. Divisions 1 and 2 are located inside the EPGB located on one side of the Reactor Building (RB), and

divisions 3 and 4 are located inside the EPGB located on the opposite side of the RB. Each division has a separate and independent HVAC system. The HVAC systems for each of the four divisions are identical.

The air intake and exhaust stack of the EPGBVS are located such that exhaust gases being drawn into the air inlet stream are limited to an insignificant level. The exhaust stack is located approximately 70 feet from the air intake, and the exhaust air flow is directed away from the air intake flow.

One of the divisions of the EPGBVS is illustrated in Figure 9.4.9-1—Emergency Power Generating Building Ventilation System. The other three divisions are identical.

The EPGBVS consists of following subsystems for each division:

- Ventilation of diesel hall.
- Ventilation of electric room.
- Ventilation of main tank room.

Ventilation of Diesel Hall

The outside air is drawn into the HVAC supply room through an air intake screen or grill which prevents large objects from entering the air intake. The fresh air intake is located approximately fifty feet above grade elevation and is protected against tornado missiles. The screen or grill is heated during the winter to prevent ice buildup.

The air from the HVAC supply room is supplied through two separate air trains which include back draft damper, prefilter, and supply fan. Each diesel hall supply and exhaust fans maintain the diesel hall temperature between 59°F and 140°F. The supply air is delivered through ductwork to the diesel hall.

An additional non-safety-related air supply and exhaust ventilation system to the diesel hall is also installed that operates when the large safety-related supply and exhaust system is not required to operate during maintenance or when the moderate outside temperature does not allow the large supply and exhaust fans to operate. The non-safety-related air supply is drawn from the HVAC supply room, the system includes an air intake screen or grill, backdraft damper, prefilter, supply fan, motor operated damper, and manual damper. The non-safety-related air exhausts to the HVAC air exhaust room, the system includes a motor operated damper, exhaust fan and backdraft damper.

The non-safety-related ventilation system prevents frequent starting and stopping of the large safety-related supply and exhaust fans. A safety-related temperature sensor in the diesel hall controls operation of one or both safety-related supply/exhaust fans as required to maintain design temperature in the diesel hall. Initially, the non-safety

fans operate, and as the diesel hall temperature increases both safety-related supply/exhaust fans start operating. Operation of safety-related fans shuts down the non-safety fans and closes the motor operated dampers. A separate safety-related temperature sensor in the diesel hall provides low/high room temperature alarm in the MCR. This sensor also closes the safety-related motor operated dampers located on the non-safety-related air supply/exhaust system when the diesel hall temperature reaches at or below 59°F.

During winter conditions, when the EDGs are not in operation, the air in the diesel hall is recirculated through four electrical ~~air~~ fan heaters. These fans are controlled by local thermostats to maintain the required minimum temperature.

The exhaust air from the diesel hall is directed to the HVAC exhaust room through two separate ducts which include an exhaust fan and a back draft damper. The exhaust plenum is split into two sections: one is for the diesel engine exhaust, and the other is for HVAC exhaust. This separation of exhaust prevents diesel exhaust back pressure from affecting the HVAC exhaust ventilation fans. This boundary prevents inadvertent entry of diesel engine exhaust into the diesel room if one of the HVAC exhaust damper fails to close. This partition also protects the HVAC equipment and improves working environment inside the area.

Ventilation of Electric Room

A non-safety-related inlet air supply for the electrical room is drawn from outside air through a motor operated damper, manual damper, prefilter, refrigerant evaporator cooler, and fan. The operation of this unit is automatically controlled by a room thermostat that maintains the electrical room temperature between 40°F and 113°F. A safety-related temperature sensor located outside under a tornado protective hood, sends a signal to open or close the safety-related motor operated damper that is located on the non-safety-related inlet air supply. This damper automatically closes when outside air temperature is below 50°F or above 100°F. This prevents entry of hot or cold outside air. The non-safety-related cooling system operates only when the EDGs are not operating. A backdraft damper is installed at the boundary of electrical room and diesel hall to allow the electrical room air to exhaust to the diesel hall.

A safety-related cooling system for the electrical room operates when the EDGs are also operating. This system recirculates the electrical room air through an air conditioning unit that consists of ~~fire dampers,~~ manual damper, prefilter, HEPA filter, cooling coil, moisture separator, and supply fan. The fan air flow maintains electrical room temperature within the design temperature limits of 40°F and 113°F. The water for the cooling coil is supplied from the ESW system. The recirculated air from the electrical room is controlled to maintain ambient conditions inside the electrical room.

Ventilation of Main Tank Room

The air supply to the main tank room is drawn from the diesel hall or HVAC supply air room through an electric louver damper, a back draft damper, and a fire damper. The exhaust air from the main tank room is directed through louver damper, exhaust fan, and a back draft damper. The exhaust air is then directed to the building exhaust through an outlet screen or grill. The exhaust fan is designed to maintain the required ventilation rate of the main tank room. The main tank room exhaust design air flow is 3,200 scfm. During winter, local heaters maintain the required minimum temperature inside the main tank room. These heaters are controlled by local thermostats.

9.4.9.2.2 Component Description

The major components of the EPGBVS are listed in the following paragraphs, along with the applicable codes and standards. Table 3.2.2-1 provides the seismic design and other design classifications for components in the EPGBVS.

Ductwork and Accessories

The supply and exhaust air ducts are constructed of galvanized or stainless steel plates or sheets, and structurally designed for fan shutoff pressures. The ductwork meets the design, testing and construction requirements of ASME AG-1 (Reference 1).

Deleted paragraph.

Electric ~~Air Heating Convectors (Area~~ Heaters~~)~~

The electric ~~area~~ heaters are installed in the main tank room to maintain room ambient conditions and controlled by local room temperature sensors. Electrical heating coils are fin tubular type and meet the requirements of ASME AG-1 (Reference 1).

Fan Heaters

Fan heaters are used in the diesel hall to maintain acceptable temperature in the area. The fan heaters include a fan and electric heater. These fan heaters are controlled by a thermostat.

Prefilters

Prefilters are located upstream of HEPA filters and on all supply air inlets. The prefilters meet the requirements of ANSI/ASHRAE Standard 52.2 (Reference 2).

HEPA Filters

HEPA filters are constructed, qualified and tested in accordance with ASME AG-1 (Reference 1). The periodic inplace testing of HEPA filters to determine the leak-tightness is performed in accordance with ANSI/ASME N510 (Reference 3).

Fans

The supply and exhaust fans are centrifugal or axial type with electrical motor drivers. Fan performance is rated in accordance with ANSI/AMCA 210~~-99~~ (Reference 4), ~~ANSI/~~AMCA 211~~-1987~~ (Reference 5), and ANSI/AMCA 300~~-1985~~ (Reference 6).

Isolation Dampers

Manual dampers are adjusted during initial plant testing to establish accurate flow balance between the rooms. The motor-operated dampers will fail ~~in the~~ "as-is"~~ position~~ in the case of power loss. Backdraft dampers prevent air flow to non-operating air supply and exhaust trains. The performance and testing requirements of the dampers are in accordance with ASME AG-1 (Reference 1).

Fire Dampers

Fire dampers are installed where ductwork penetrates a fire barrier. Fire damper design meets the requirements of ~~UL 555~~ NFPA 80 (Reference 7) and NFPA 90A (Reference 11) and the damper fire rating is commensurate with the fire rating of the barrier penetrated. ~~The fire dampers are included in the discussion of the EPGB fire protection system (refer to Appendix 9A.3.6).~~ Fire dampers are equipped with fusible links for automatic closure when the temperature reaches a predetermined setpoint.

Cooling Coils

Cooling coils are installed in the supply and recirculation train for cooling of the electrical room. The cooling coils are of finned tube coil type and designed in accordance with ASME AG-1 (Reference 1). The coil in the non-safety air cooling system is cooled using a refrigerant evaporator cooler. The safety recirculation cooling coil is cooled by the ESW system.

Moisture Separator

The moisture separator is installed in the air conditioning train to collect condensate, which is directed to the drain system.

9.4.9.2.3 System Operation

Normal Plant Operation

The EPGBVS maintains acceptable ambient conditions in the diesel hall, electric room, and main tank room of each of the four EPGB divisions. During normal plant operation, the EDGs do not operate. However, outside air is supplied to the diesel hall to maintain an acceptable ambient temperature for the startup of the EDGs and personnel comfort. In winter conditions, four fan heaters are available to maintain the required minimum temperature in the diesel hall. When the EDGs are in operation,

the exhaust air removes the heat generated in the diesel hall. The operation of air supply fans and the opening of dampers depend on the diesel hall temperature detected by the sensors. The diesel hall temperature is kept in the appropriate band by controlling the position of dampers and operating the air supply fans.

Air renewals for the diesel hall and main tank room are maintained as needed to obtain the required ambient temperatures. The non-safety-related split system air conditioner supplies the electrical room with outside air that is mixed with the recycled air from the electrical room. The mixed air is then processed through the air conditioning train and supplied to the electrical room. The safety-related ESW cooling unit will operate only when the EDGs are operating or during the tests of EDGs.

The main tank room is ventilated by air supplied from the HVAC supply air room or diesel hall. The main tank room air is discharged through the exhaust duct to an exhaust fan and then out of the building. The main tank room is heated by a local electric heater, which is activated by a thermostat to maintain a minimum required room temperature.

Fire dampers are located on the ventilation system to avoid fire propagation in the building. The rooms are completely isolated in case of a fire in the room. ~~Fire is detected by a fire alarm system which automatically closes the corresponding fire damper.~~

Abnormal System Operating Conditions

Failure of Diesel Hall Air Supply

If one or more components of the diesel hall supply air fail, the EPGBVS is not able to maintain the required ambient conditions. At lower outside temperature, the system uses only one supply fan to provide sufficient ventilation for the proper operation of the EDGs. Since there are four redundant EPGB divisions, the failure of the diesel hall air supply in one division does not affect the other three divisions.

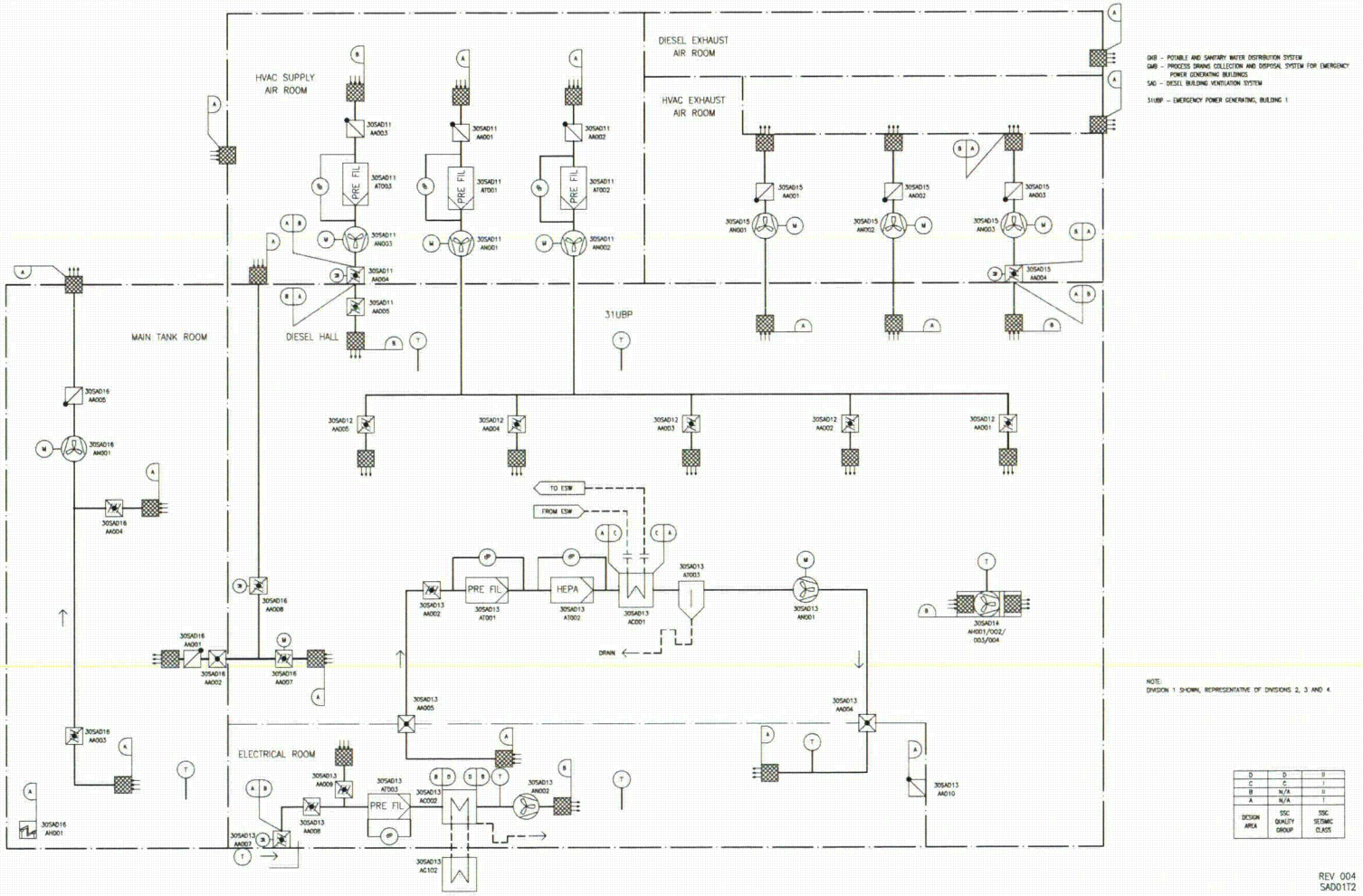
Failure of Diesel Hall Fan Heater

The diesel hall has four fan heaters. In the case of failure of one heater fan, the other three fans are able to maintain the required temperature in the diesel hall.

Failure of Electric Room Safety-Related Air Cooling Unit

In the case of failure of a component on the safety-related air conditioning train for the electric room, the required ambient conditions are not maintained in the electric room when EDG is operating. However, other unaffected divisions are available to provide necessary power during this event.

Figure 9.4.9-1—Emergency Power Generating Building Ventilation System



Next File

9.4.11 Essential Service Water Pump Building Ventilation System

The essential service water pump building ventilation system (ESWPBVS) provides conditioned air to the essential service water system (ESWS) pump areas and associated electrical equipment areas. The ESWPBVS provides an environment suitable for the operation of the ESWS pumps (refer to Section 9.2.1) and associated electrical equipment by maintaining acceptable temperature conditions in each of the four ESWS Pump Buildings. Each building has its own independent ventilation system and is not connected to the other buildings.

9.4.11.1 Design Bases

The ESWPBVS consists of a safety-related cooling system and room air heaters and a non-safety related cooling unit. The safety-related portion is designed to Seismic Category I criteria. The non-safety-related portion is designed to Seismic Category II. The ESWPBVS performs the following safety-related system functions and complies with the general design criteria (GDC) indicated below:

- The ESWPBVS maintains acceptable temperature limits to support operation of the ESWS pumps that are required to operate during design basis accident conditions. The ESWPBVS maintains a minimum temperature of 41°F and a maximum temperature of 113°F in the ESWS Pump Buildings for personnel accessibility and to support operation of the ESWS pumps. This temperature range maintains a mild environment in these buildings, as defined in Section 3.11.

- The ESWPBVS components are located inside the ESWS Pump Buildings, which are designed to withstand the effects of natural phenomena, such as earthquakes, tornadoes, hurricanes, floods, and external missiles (GDC 2).

- The ESWPBVS components are appropriately protected against dynamic effects and designed to accommodate the effects of, and to be compatible with, the environmental conditions associated with normal operation, maintenance, testing and postulated accidents. The components of the ESWPBVS remain functional and perform their intended safety function after anticipated operational occurrences and design basis accidents, such as a fire, internal missiles, or pipe break (GDC 4).

- The safety-related components and systems of the ESWPBVS are not shared among nuclear power units (GDC 5).

- The essential onsite electrical power systems meet the guidance of NUREG-CR/0660 (Reference 1) (subsection A–item 2, and subsection C-item 1) for protection of essential electrical components (such as contactors, relays, circuit breakers) from failure due to the accumulation of dust and particulate materials (GDC 17).

- Power and control functions are designed in accordance with RG 1.32.

Air conditioning and heating loads for the ESWS pump rooms are calculated using methodology identified in ASHRAE Handbook (Reference 8).

- Summer air conditioning loads will be calculated with a maximum outside air design temperature 0 percent exceedance value, using U.S. EPR Site Design Envelope Temperature (See Table 2.1-1). The analysis will be completed for both a normal and accident plant alignment configuration.
- The safety-related cooling supply units are designed to provide cooling as required to prevent the ESWS pump room temperatures from exceeding their maximum design temperature.
- Winter heating loads will be calculated with the plant operating in an outage alignment configuration. Winter heat loads will be calculated with a minimum outside air design temperature 0 percent exceedance value, using U.S. EPR Site Design Envelope Temperature (See Table 2.1-1).

The ESWPBVS performs the following non safety-related system functions:.

- Provides outside air and cooling to the ESWPB when the ESW pumps are not operating.

9.4.11.2 System Description

9.4.11.2.1 General Description

A drawing of the ESWPBVS applicable to each of the four ESWS Pump Buildings is shown in Figure 9.4.11-1—Essential Service Water Pump Building Ventilation System.

The ESWPBVS supplies the recirculation air for cooling or heating of the ESWS pump area and electrical equipment area located inside each of the four ESWS Pump Buildings. Each building has its own independent ventilation system.

This ventilation system is not expected to contain or interface with any radioactive materials, and so is not considered an Engineered-Safety-Feature Atmospheric Clean-Up System.

Safety-Related Cooling and Heating

The safety-related cooling units operate when the ESW pump is operating in that building. Room air is drawn through an air inlet grill and processed through an air conditioning train. The conditioned air is supplied to the ESWS pump area and electrical equipment area. The room air is then returned to the air conditioning train. The air conditioning train for each building is comprised of the following components:

- Recirculation supply air ductwork.

- Manual balancing damper.
- Prefilter.

Each ESWPB has two safety-related room air heater units to prevent freezing within the ESW pump rooms during winter.

- Cooling coils, which cool the recirculation air to the required supply air temperature, have a total cooling capacity of 619,400 Btu/hr. The cooling coils are supplied with water from the ESWS pump and the water is discharged into the respective cooling tower basin. Manual isolation valves are provided to isolate the cooling coils for maintenance.
- Moisture separator, which drains the condensate to the cooling tower basin.
- Heaters, which heat the recirculation air during winter conditions to maintain the minimum required temperature.
- Supply air recirculation fans, are designed to provide an air flow rate of 30,000 scfm.
- Supply air louver dampers.
- Motor operated outside air inlet and outlet isolation dampers.

Non-Safety Related Cooling Unit

The non-safety-related cooling units in each pump house pull in outside air through a grille protected by a tornado barrier. The outside air is mixed with recirculated room air through balancing dampers and processed through an air conditioning train. The non-safety-related air conditioning train for each building is comprised of the following components:

- Supply ducting with bird screen.
- Manual balancing dampers.
- Prefilters.
- Split system refrigerant air conditioning cooling coil.
- Supply air fan.

9.4.11.2.2 Component Description

The major safety-related components of the ESWPBVS are listed in the following paragraphs, along with the applicable codes and standards. Table 3.2.2-1 provides the seismic design and other design classifications for components in the ESWPBVS.

Ductwork and Accessories

The supply air duct is constructed of galvanized sheet steel and is structurally designed for the fan shutoff pressure. The ductwork meets the design, construction and testing requirements of ASME AG-1 (Reference 2).

Cooling Coils

The cooling coils are designed in accordance with ASME AG-1 (Reference 2).

Cooling Coil Isolation Valves

The cooling coil isolation valves are designed to meet ASME Boiler and Pressure Vessel Code, Section III, Class 3 (Reference 7).

Moisture Separators

Deleted paragraph.

Each moisture separator is installed to collect the condensate which is directed to the cooling tower basin.

Air Supply Fan

The fan is centrifugal or axial type with an electrical motor driver. Fan performance is rated in accordance with ANSI/AMCA 210 (Reference 4), ~~ANSI/~~AMCA 211 (Reference 5), and ANSI/AMCA 300 (Reference 6).

Balancing Dampers

Manual dampers are adjusted during initial plant testing to establish an accurate flow balance. The performance and testing requirements of the dampers are per Reference 2.

Motor Operated Isolation Dampers

The motor operated isolation dampers will fail as-is ~~in position~~ in case of power loss. The outside air inlet/outlet motor operated isolation dampers are designed to ASME AG-1 (Reference 2) damper isolation leakage class II requirements.

Electric Heaters

The electric heaters meet the requirements of ASME AG-1 (Reference 2).

9.4.11.2.3 System Operation

Normal Plant Operation

During normal plant operation, the non-safety-related cooler maintains the ESW Pump Room between 50°F and 100°F, during summer months when the ESW pumps

are not in operation. The safety-related cooler for a particular ESWPB will operate when the ESW pump in that building is in operation. The non-safety-related cooler can operate concurrent with the safety-related cooler with or without the ESW pumps in operation. A safety-related temperature sensor (located outside under the tornado protective hood for inlet outside air) sends a signal to open or close the safety-related inlet and outlet motor operated isolation dampers when the outside air temperature is above 100°F or below 50°F. This will prevent the entry of the hot or cold outside air, which could allow the temperature in the ESW building to fall above or below the maximum/minimum design temperature of 113°F/41~~0~~°F.

During winter, the room air is heated by two safety-related wall mounted electric heaters. Local thermostats start and stop the safety-related heater units to maintain the ESW pump room temperature between 50°F and 100°F.

Abnormal Operating Conditions

If one or more components of the ESWPBVS fail, the ESWPBVS is not able to maintain the required ambient conditions in the affected building. Because there are four independent ESWS pump buildings, the failure in one building does not affect the other three buildings.

Loss of Off-Site Power

In the event of loss of offsite power (LOOP), the safety-related ESWPB cooling system and room air heaters continue to operate. The power is supplied from the Class 1E emergency power supply system (EPSS).

Station Blackout

In the event of station blackout (SBO), the ESWPBVS is not operable.

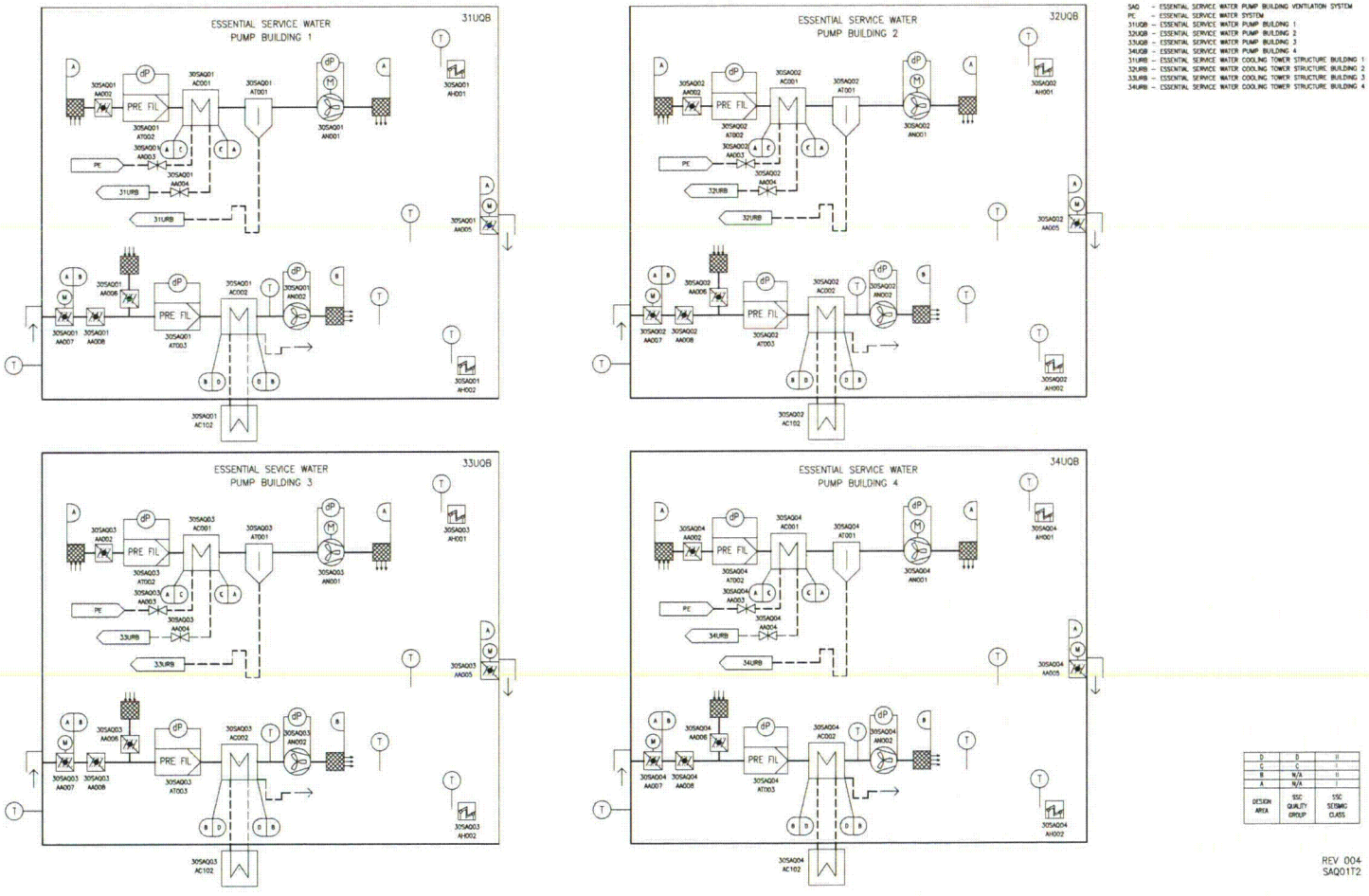
Plant Accident Conditions

The safety-related ESWPB cooling system and room air heaters are required to operate during design basis accident conditions. Even if the ESWS pumps are not required to operate, the safety-related ESWPBVS maintains conditions in the ESWS pump buildings in case the ESWS pumps are required to operate.

9.4.11.3 Safety Evaluation

The ESWPBVS has sufficient cooling capacity to maintain the pump room temperature below 113°F when the ESWS pump motors are operating at rated load and the outside air is at the maximum site design ambient temperature of 115°F. The heater is controlled by a local temperature control system having a predetermined temperature setpoint.

Figure 9.4.11-1—Essential Service Water Pump Building Ventilation System



Next File

5.1.6 The operation of the SBVS recirculation cooling units meets design requirements.

5.1.7 SBVS alarms, indicating lights and status lights meet design requirements.

5.1.8 SBVS meets duct/housing total leakage requirements.

5.2 Verify that safety-related components meet electrical independence and redundancy requirements.

5.3 ~~The SBVS meets design requirements to monitor radiation (refer to Table 11.5-1, Monitors R-25 and R-26).~~

5.4 Radiation monitoring instrumentation meets design requirements to monitor radiation and respond as designed to radiation sources (refer to Table 11.5-1, Radiation Measuring Points R-25 and R-26). This includes, but is not limited to, the following that could adversely impact the ability to measure the parameters described in Table 11.5-1:

5.4.1 Range.

5.4.2 Response time.

5.4.3 Sensitivity.

5.5 Radiation monitoring instrumentation meets design requirements to monitor radiation and initiate Automatic Control Functions (refer to Table 11.5-1, Radiation Measuring Point R-25) upon detection of high activity levels.

5.5.1 For each applicable radiation monitor, the response time from the radiation monitor reaching the level to initiate the automated control function until each actuated component has reached the required position meets the design requirement.

5.6 Radiation sample points (refer to Table 11.5-1, Radiation Measuring Points R-25 and R-26) are capable of collecting the required samples.

14.2.12.8.12 Emergency Power Generating Building Ventilation System (Test #084)

1.0 OBJECTIVE

1.1 To demonstrate proper operation of the emergency power generating building ventilation system (EPGBVS).

1.2 To demonstrate proper operation of the EPGBVS.

1.3 To demonstrate electrical independence and redundancy of power supplies.

2.0 PREREQUISITES

2.1 Construction activities on the EPGBVS have been completed.

2.2 EPGBVS instrumentation has been calibrated and is operating satisfactorily prior to performing the following test.

2.3 Support systems required for operation of the EPGBVS are complete and functional.

2.4 Test instrumentation is available and calibrated.

3.0 TEST METHOD

3.1 Verify control logic.

3.2 Verify design air flow with each EPGBVS in operation.

3.3 Verify design temperature can be maintained in each Emergency Power Generating Building.

3.4 Verify alarms, indicating instruments, and status lights are functional.

3.5 Check electrical independence and redundancy of power supplies for safety-related functions by selectively removing power and determining loss of function.

3.6 Verify that operation of dampers meet the requirements of ASME AG-1.

3.7 Verify that duct/housing leakage requirements are met.

4.0 DATA REQUIRED

4.1 Fan and damper operating data.

4.2 Air flow verification

4.3 Setpoint at which alarms, interlocks, and controls occur.

4.4 Temperature data of each Emergency Power Generating Building.

5.0 ACCEPTANCE CRITERIA

5.1 The EPGBVS operates as designed (refer to Section 9.4.9):

5.1.1 EPGBVS alarms, interlocks, protective devices, and controls (manual and automatic) function as designed.

5.1.2 EPGBVS fan performance meets design requirements.

5.1.3 EPGBVS dampers/valve performance (i.e., thrust, opening times, closing times, and ability to control flow) meets design requirements.

5.1.4 EPGBVS air balance meets design requirements.

5.1.5 EPGBVS meets duct/housing total leakage requirements.

5.2 Verify that safety-related components meet electrical independence and redundancy requirements.

3.2 Verify design air flow of each fan.

3.3 Verify alarms, indicating instruments and status lights are functional.

3.4 Verify design temperatures can be maintained in the structure.

3.5 Check electrical independence and redundancy of power supplies for safety-related functions by selectively removing power and determining loss of function.

3.6 Verify that operation of isolation dampers meet the requirements of ASME AG-1.

3.7 Verify operation of the electric air convectors (area heaters).

4.0 DATA REQUIRED

4.1 Temperature data for the structure from each fan unit.

4.2 Air balancing report, including fan operating data.

4.3 Setpoints at which alarms and interlocks occur.

5.0 ACCEPTANCE CRITERIA

5.1 The ESWPBVS operates as designed (refer to Section 9.4.11):

5.1.1 ESWPBVS alarms, interlocks, protective devices, and controls (manual and automatic) function as designed.

5.1.2 ESWPBVS fan performance meets design requirements.

5.1.3 ESWPBVS dampers/valve performance (i.e., thrust, opening times, closing times, and ability to control flow) meets design requirements.

5.1.4 ESWPBVS air balance meets design requirements.

5.1.5 ESWPBVS electric air heaters meet design requirements.

5.2 Verify that safety-related components meet electrical independence and redundancy requirements.

14.2.12.8.17 Main Steam and Feedwater Valve Room System (Test #089)

1.0 OBJECTIVE

1.1 To demonstrate that the main steam and feedwater valve room ventilation system (VRVS) provides a suitable operating environment for equipment and personnel during normal operations.

2.0 PREREQUISITES

2.1 Construction activities on the VRVS have been completed.

2.2 VRVS instrumentation has been calibrated and is operating satisfactorily prior to performing the following test.

2.3 Support systems required for operation of the VRVS are complete and functional.

ANP-10309NP – U.S EPR Protection System Technical Report Markups

Table 7-1—Modification of Voting Logic Towards Actuation

Voting Type	Faulty Inputs	Result
2 out of 4 3 out of 4	0	2 out of 4 3 out of 4
	1	2 out of 3
	2	1 out of 2
	3	Actuation
	4	Actuation
2 out of 8	0	2 out of 8
	1	2 out of 7
	2	2 out of 6
	3	2 out of 5
	4	2 out of 4
	5	2 out of 3
	6	1 out of 2
	7	Actuation
	8	Actuation
2 out of 3	0	2 out of 3
	1	1 out of 2
	2	Actuation
	3	Actuation
1 out of 4	0	1 out of 4
	1	Actuation
	2	Actuation
	3	Actuation
	4	Actuation
1 out of 2	0	1 out of 2
	1	Actuation
	2	Actuation

- ~~0 faulty input signals: Vote is 2/4.~~
- ~~1 faulty input signal: Vote is 2/3.~~
- ~~2 faulty input signals: Vote is 1/2.~~
- ~~3 faulty input signals: Actuation.~~
- ~~4 faulty input signals: Actuation.~~

When an invalid signal is received by "functional AND" logic, the signal is ignored. For example, a "functional AND" logical operation with four inputs requires that all four inputs be TRUE to obtain a TRUE output. When an invalid signal is input to this operation, only the remaining three valid inputs must be TRUE to obtain a TRUE output.

Likewise, when an invalid signal is received by "functional OR" logic, the signal is ignored. For example, if a "functional OR" logical operation with four inputs requires that any one of the four inputs must be TRUE to obtain a TRUE output. When an invalid signal is input to this operation, only one of the remaining three valid inputs must be TRUE to obtain a TRUE output.

Further information concerning the identification of invalid signals in a TXS-based system is provided in Reference 24.

7.4 *Reactor Trip Outputs*

The RT outputs of the two redundant ALUs in a subsystem are combined in a hardwired "functional AND" configuration. This requires both ALUs to output the RT order for the associated RT device to be actuated. The outputs of the "functional AND" from both subsystems within a division are combined in a "functional OR" logic. These configurations are shown in Figure 7-2.

The RT devices used by the PS are de-energize to actuate (i.e., the PS outputs must be in a zero-voltage state to actuate the RT). The normal state of the RT outputs is a high-voltage state, maintaining the trip devices in a closed position.

The term "functional AND" describes the logical operation where both inputs must be in a zero-voltage state to obtain a TRUE output. The TRUE output corresponds to a zero-voltage state.

- The actuation signal is latched via a memory logic block with set-reset priority ~~function block~~ in the ALU to confirm completion of the function. (See Figure 7.1-1 of the U.S. EPR FSAR and the definitions in Section 7.1 of the U.S. EPR FSAR.)~~.~~

- The ESF actuation signals of the redundant ALUs in each subsystem are combined in a hardwired "functional OR"; therefore, either of the redundant ALUs can actuate an ESF function. The result of the "functional OR" is an ESF actuation order.

8.2 *ESF Actuation Voting Logic*

Single failures upstream of the ALU layer that could result in an invalid signal being used in the ESF actuation are accommodated by modifying the vote in the ALU layer. Each ESF actuation function is evaluated on a case-by-case basis to determine whether the vote is modified toward actuation or no actuation. In cases where inappropriate actuation of an ESF function could challenge plant safety, the function is modified toward no actuation. Otherwise, the function is modified toward actuation. The EDG Actuation and MCR Air Conditioning System Isolation and Filtering functions are the only ESF actuation functions that are modified towards actuation. All other ESF actuation functions are modified towards no actuation. The concept of modification toward actuation is described in Section 7.2. The concept of modification toward no actuation based on the number of input signals to the voting function block that carry a faulty status is as follows~~:~~.

Table 8-1—Modification of Voting Logic Towards No Actuation

Voting Type	Faulty Inputs	Result
2 out of 4 3 out of 4	0	2 out of 4 3 out of 4
	1	2 out of 3
	2	2 out of 2
	3	No Actuation
	4	No Actuation
2 out of 3	0	2 out of 3
	1	2 out of 2
	2	No Actuation
	3	No Actuation
1 out of 2	0	1 out of 2
	1	1 out of 1
	2	No Actuation

- ~~0 faulty input signals: Vote is 2/4.~~
- ~~1 faulty input signal: Vote is 2/3.~~
- ~~2 faulty input signals: Vote is 2/2.~~
- ~~3 faulty input signals: No actuation.~~
- ~~4 faulty input signals No actuation.~~

Section 7.3 describes the methods used to mark an invalid signal with a faulty status before reaching the voting function.

8.3 *ESF Actuation Outputs*

Each ESF actuator can receive actuation orders from multiple I&C systems. Therefore, the priority and actuation control system (PACS) is used to prioritize the actuation orders. The PACS collects the actuation signals from multiple I&C systems and transfers the proper actuation order to the actuator according to pre-defined priority assignments.

11.0 INTERCHANNEL COMMUNICATION

11.1 *Communication Interfaces*

The use of interchannel communication in ~~the PS~~TXS systems is demonstrated by communication between two function processors located in two different divisions of ~~the PS~~TXS systems (Figure 11-1). The typical hardware configuration includes a function processor with a process field bus (PROFIBUS) communication module attached. Each communication module is connected to an OLM that converts the electrical communication signals to optical signals, which are transmitted over fiber-optic cables to other OLMs on the network.

Communication activities are performed sequentially and controlled by the central control unit of the runtime environment. The sending function processor initiates sending activities and the messages are addressed to the receiving function processor. The intermediate communication modules and OLMs transfer the messages without influencing the message data. The dual port random access memory (DPRAM) contained in the communication module serves as a buffering circuit and separates data flow between send and receive channels. The separation of data flow is continued within the function processor by the message input and message output buffers. The function processor accesses the DPRAM independently of access by the communication module's PROFIBUS controller, which sends and receives data to and from the network.

11.2 *Communications Independence*

The TXS platform is designed using principles to provide communication independence. These principles are referred to as principles for interference-free communication in Reference 23. These principles, which provide communication independence between the redundant divisions of the ~~PS~~ TXS systems, are summarized as follows:

Guidance in IEEE Std 7-4.3.2 is supplemented by an annex on communication independence (Reference 14), which defines acceptable means for functional unit communications between redundant divisions and between safety and non-safety systems.

The TXS communication techniques provide communication independence between redundant divisions and are consistent with the guidance in Reference 14. The related figure from Reference 14 is duplicated in Figure 11-2. An equivalent figure describing the TXS communication is shown in Figure 11-3. Figure 11-3 depicts the use of buffering circuits and separation of data flow (communication isolation), which provide an acceptable method of communication independence and prevents adverse interactions.

For communication between redundant divisions in the ~~PS~~ TXS systems, the buffering circuit consists of the PROFIBUS controller and the DPRAM; both are contained in the communication module. The communication module provides buffering so the function processors can read and write to the DPRAM independently of the PROFIBUS controller, which transfers data between the network and the DPRAM. Therefore, the function processor in one division operates independently of the operation of a function processor in a redundant division.

The DPRAM also begins the separation of data flow, which continues inside the function processor. Within the function processor, messages from the receive portion of the DPRAM are transferred to the message input buffers where data validation is performed before the data is used in function diagram processing. The results of function diagram processing are placed in the message output buffers (separate from the input buffers), for transfer to the send portion of the DPRAM. This separation of data flow constitutes communication isolation.

The DPRAM contributes to communication independence in two ways:

- It acts as a buffering feature that allows the function processor to operate independently from the PROFIBUS controller.

EPR FSAR Tier 2, Section 7.2 and Section 7.3, are used as the bases for the analysis. This FMEA follows the guidance of the U.S. EPR general engineering guideline for failure modes and effects analysis. After detailed hardware layout and application specific software documentation are produced, the performance of a detailed FMEA is required to confirm the results of the system-level FMEA.

Per Reference 1, the essential function of an FMEA is to consider each major part of the system, how it may fail (the mode of the failure) and what the effect of the failure on the system would be (the failure effect). To define the major parts of the system for which failures are assumed, a single division of the PS is divided into functional units as described in Section 5.0. The PS consists of four identical divisions, so the definition of functional units is the same for each division. In general, a single failure of the same unit in any of the four PS divisions has the same effect on every function processed by that unit, regardless of which division has the failed unit. Therefore, the failure of each functional unit in one division is analyzed and considered representative of the effects of the same failure in any other division. Any exceptions are identified.

The FMEA contained herein is prepared in support of the U.S. EPR Design Certification Document submittal. It consists of an FMEA of the parts of the system that participate in the generation of automatic reactor trip (RT), engineered safety features actuation system (ESFAS), interlock, and permissive signals. The functional units that are analyzed are the following:

- Acquisition and processing units (APU)
- Actuation logic units (ALU)

In addition to the equipment defined as functional units of the system, certain other equipment also contributes to the automatic RT, ESFAS, interlock, and permissive functions and is analyzed as part of the system-level FMEA:

- Sensor input measurements from the SCDS
- Hardwired output logic

- The P18 permissive is validated from an RT initiation signal. The FMEA for the P18 permissive validation on an RT initiation will be covered by the FMEA for the RT functions.

- The P6 permissive and P13 permissive are unique in that the inhibited state of the permissive enables the associated protective functions. It is, therefore, desirable to have the permissive fail into the inhibited state. Therefore, the voting logic used in the P6 and P13 permissives is modified toward inhibition (state is "0") of the permissive in case of invalid input signals as follows:

Table A.1-2—Voting Logic for P6 and P13 Permissives

		Initial Voting Logic
		3/4
# of invalid inputs	1	2/3
	2	2/2
	3	Output = "0"
	4	Output = "0"

The voting logic for all permissives, other than P6 permissive and P13 permissive, is modified toward validation (state is "1") in case of invalid input signals as follows:

Table A.1-3—Voting Logic for other Permissives

		Initial Voting Logic		
		2/3	2/4	3/4
# of invalid inputs	1	1/2	2/3	2/3
	2	Output = "1"	1/2	1/2
	3	Output = "1"	Output = "1"	Output = "1"
	4		Output = "1"	Output = "1"

- For the MHSI large miniflow valves interlock function it is desirable to have the MHSI large miniflow valves fail as-is. Therefore, the function is modified towards

no actuation in case of invalid input signals.~~AND logic and OR logic use passive status processing. That is, if one input is invalid, the output is invalid regardless of the status of the remaining inputs.~~

- There are two general cases where multiple sensors are used as inputs to a calculation:
  - The multiple inputs are redundant measurements of the same process parameter.
    - In this case, if any one input has an invalid status, that input is disregarded and the calculation is performed using the remaining inputs.
  - The multiple inputs are not redundant to one another and measure different process parameters.
    - In this case, if any one input has an invalid status, the output of the calculation is invalid.

A.2 System Description

Section A.2 provides basic information pertinent to understanding the results of the FMEA. The automatic RT, interlock, and ESFAS functions performed by the system are described in U.S. EPR FSAR Tier 2, Section 7.2, ~~and Section~~ 7.3, and 7.6.

A.2.1 Protection System Architecture

The architecture of the U.S. EPR™ Protection System can be found in U.S. EPR FSAR Tier 2, Figure 7.1-6. The four partitions on the figure represent the four physically separated, redundant PS divisions. The equipment assigned to each PS division is located in the corresponding Safeguard Building. Each PS division is further divided into subsystems A and B. The following sections identify features of the PS design that prevents a single failure from impairing the ability of the system to perform its safety functions.

Physical Separation

The four redundant divisions of the PS are physically separated within their respective Safeguard Buildings. In addition to the spatial separation features, Safeguard Building 2 and 3 are designed to protect against external hazards. The four divisionally separated rooms containing the PS equipment are in different fire zones. Therefore, the consequences of internal hazards (e.g., fire) would impact only one PS division.

Power Supply Independence

Each PS division is supplied by the independent Class 1E emergency uninterruptible power supply (EUPS). The EUPS are backed by the emergency diesel generators to cope with loss of offsite power. Inside a division, the PS cabinets are supplied by two redundant, uninterruptible 24 VDC feeds. To cope with loss of onsite and offsite power, the uninterruptible feeds to the PS cabinets are supplied with two-hour batteries.

Loss of Power

In case of loss of offsite power, each PS division is supplied with its own battery until the emergency diesel generators are started and connected to the EUPS. A single failure of a divisional battery could result in loss of power to a PS division. In that case, all function processors in the division shutdown (no data communication is sent from the division) and all outputs go to a "0" state. This results in opening that divisions RT devices (the tripped state), and no actuation of ESFAS and interlock components controlled by that division. The other 3 PS divisions remain capable of performing their protective functions. Upon restoration of power to a PS division, all function processors go through a reset and start-up self-test mode, during which the outputs remain in a "0" state. Upon successful completion of the start-up self-test, each function processor enters its normal cyclic operation mode. The RT outputs will transition from the "0" state (trip) to their normal "1" state (no-trip). This alone does not return the affected RT breaker to its normal state. Manual action is required locally (re-rack the breaker) to return to its closed position. Upon successful completion of the start-up self-test, when each function processor enters its normal cyclic operation mode, ESFAS and interlock

outputs remain in their normal "0" state. If an AOO or PA is in progress during restoration of power, a change of state of the ESFAS and interlock outputs (to the actuate state) occur to respond to the event.

Redundancy

The PS architecture is generally four-fold redundant for both RT and ESFAS functions. A single failure during corrective or periodic maintenance (maintenance bypass), or a single failure and the effects of an internal hazard do not prevent performance of the safety functions. Where there are exceptions because of limited redundancy of plant systems actuated by the PS, plant technical specifications are used to strictly limit the amount of time the related components can be out of service for maintenance. The plant technical specification controls preclude the need to consider a single failure concurrent with a maintenance condition for these cases.

For RT functions, each PS division actuates one redundancy of the RT devices based on redundant processing performed in four divisions. For ESFAS functions, the redundancy of the safety function as a whole is defined by the redundancy of the ESF system mechanical trains. In general, this results in one PS division actuating one mechanical train of an ESF system based on redundant processing performed in four divisions. The PS not only supports the redundancy of the mechanical trains, but also enhances this redundancy through techniques (e.g., redundant actuation voting).

Subsystems

Each PS division is divided into two functionally independent subsystems: A and B. Subsystem A in each division is redundant to subsystem A of the other divisions; the same is true of subsystem B. The primary purpose of this arrangement is to provide functional diversity for RT functions; however, in some cases redundancy within a division is achieved by implementing the same function in each subsystem

automatically un-latch actuation outputs. Each ALU consists of a function processor, input and output modules, and communication modules.

Each PS division contains four ALUs; two assigned to each subsystem. The two ALUs of the same subsystem within a division are redundant and perform the same processing using the same inputs. The outputs of two redundant ALUs are combined in a hardwired "functional AND" logic for RT outputs and in a hardwired "functional OR" logic for ESFAS and interlock function outputs. This avoids both unavailability of ESFAS actuations, interlock functions, and spurious RT actuations. The actuation orders from the ALU are sent to the PACS for ESFAS actuations and interlock function, or to the trip devices for RT actuations.

A.2.3 Diversity of Reactor Trip Mechanism

The PS uses two diverse, safety-related means of initiating a reactor trip: trip breakers and trip contactors. Automatic RT orders issued by the PS act on these two different safety-related components of the control rod drive power supply system, each independent and capable of actualizing the full RT.

The automatic orders to the trip devices from the PS are de-energize to actuate. This removes the power to the control rod grippers and allows the rods to drop and initiate the reactor trip.

Trip Breakers

Each PS division is assigned to one of four trip breakers; each divisional RT order acts on the under-voltage coil of the assigned breaker (de-energize to open). PS divisions 1 and 2 open trip breakers located in division 2. PS divisions 3 and 4 open trip breakers located in division 3. The trip breakers are arranged in a "1 out of 2 taken twice" configuration that withstands single failure and requires the following logical combination of PS divisional RT orders to actuate an RT: (1 or 2) and (3 or 4).

Trip Contactors

There are 23 sets of four trip contactors. Each set can remove power to four CRDM power supplies. Eleven sets of contactors are in division 1, and 12 sets are in division 4. Each PS division is assigned to one contactor in each of the 23 sets. Each set of four contactors is arranged in a 2 out of 4 configuration. Together the trip breakers and trip contactors withstand single and double failures. Additionally, the trip contactors are diverse from the trip breakers to add reliability to the reactor trip function as a whole.

A.3 Results

A.3.1 FMEA Results Definitions

The following are definitions for the items listed in Table A.3-1 through A.3-14:

1. Name of Sensor, Functional Unit, or Equipment – Each item in the PS is identified by name. The analysis was conducted at this level.

2. Associated RT – The associated reactor trip function(s) affected by the failure.

3. Associated ESFAS or interlock – The associated engineered safety features or interlock function(s) affected by the failure.

4. Failure Mode – Significant failure modes, including both random and degradation failures of the PS, are identified and evaluated.

   - Detected Failure – A failure that is automatically detected by the inherent and engineered monitoring mechanisms of the system. Detected failures of sensors or APUs result in the downstream voting logic being modified.

   - Undetected Failure – A failure that is not automatically detected by the system. Undetected failures are detectable through periodic testing. An undetected failure of a sensor or APU results in the downstream voting logic inherently becoming different.

5. Effect of a Division out for Maintenance (Tables A.3-2 through A.3-14 only) – The effects on the PS from a division taken out for maintenance, and all of the components within that division made inoperable.

6. Failure Cause – The failure cause is not identified in the system-level analysis. The failure modes are selected to bound the results of any specific failure cause. Specific failure causes can be identified only after specific equipment is selected and application software is developed.

7. Method of Detection – For the system-level FMEA, the method of detection (for detectable failures) is always inherent or engineered monitoring mechanisms. Specific methods of detection cannot be identified until specific equipment is selected and application software is developed.

8. Inherent Compensating Provision(s) – This entry lists the existing provisions within the system that compensates for the failure mode at the level being analyzed.

9. Effect on the Protection System – This entry lists the ultimate effect on the PS.

10. Comments – This entry lists any other effects, outcomes or general information related to the failure.

A.3.2 RT, Interlock, and ESF Functions Results

The results of the U.S. EPR PS FMEA for RT, interlock and ESFA functions are shown in Table A.3-1.

Table A.3-1—FMEA Results Table

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS or Interlock	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
1	Incore Detector (SPNDs)	RT-HLPD RT-Low DNBR	None	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed SPND marked invalid	For a detected failure of 1 to 5 SPNDs, the PS degrades the setpoint to compensate for the failure. On 6th invalid SPND, technical specifications dictate reduction in power to mode where SPND are not required. 7 or more invalid SPND result in automatic RT.	The undetected failure of the most limiting SPND signal is analyzed as a credible single failure in the Chapter 15 safety analyses (U.S. EPR FSAR Tier 2, Chapter 15).
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	Specific consideration as a single failure in the safety analyses	No effects on the system level.	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Safety analysis credits the undetected failure of an SPND.	No effects on the system level.	
2	Excore Detector (PRDs)	RT-High neutron Flux rate of change	None	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS or Interlock	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
31	MCR Intake Activity	None	MCR Air Conditioning System Isolation and Filtering	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	The MCR Air Intake System shall go into filtration mode (Reconfigure Air Intake). This is a safe state for the system.	The MCR Air Intake System shall go into filtration mode (Reconfigure Air Intake) if a radiation monitor fails or is put into maintenance.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/3 voting	Affected division issues spurious partial trigger; the MCR Air Intake System shall go into filtration mode (Reconfigure Air Intake). This is a safe state for the system.	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 1/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 1/2	
32	RHR 1st RCPB Isolation Valve Closed	None	MHSI Large Miniflow Valves Interlock Between P14 and P17 Permissives	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid	Downstream voting logic modified to 1/1. No effects on the system level.	If a division is inoperable then the MHSI large miniflow valve for that respective train is inoperable. The RHR safety valves will provide overpressure protection of the RHR system.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/2 and 2/3 voting	Downstream voting logic sends an actuate signal. Downstream AND logic prevents the failure from actuating the valve. No effects on the system level.	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	1/2 and 2/3 voting	Downstream voting logic becomes 1/1. No effects on the system level.	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS or Interlock	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
33	RHR 2nd RCPB Isolation Valve Closed	None	MHSI Large Miniflow Valves Interlock Between P14 and P17 Permissives	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid	Downstream voting logic modified to 1/1. No effects on the system level. No effects on the system level.	If a division is inoperable then the MHSI large miniflow valve for that respective train is inoperable. The RHR safety valves will provide overpressure protection of the RHR system.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/2 and 2/3 voting	Downstream voting logic sends an actuate signal. Downstream AND logic prevents the failure from actuating the valve.	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	1/2 and 2/3 voting	Downstream voting logic becomes 1/1. No effects on the system level.	
34	RHR Outside Containment Isolation Valve	None	MHSI Large Miniflow Valves Interlock Between P14 and P17 Permissives	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid	Downstream voting logic modified to ~~1~~2/2. No effects on the system level.	If a division is inoperable then the MHSI large miniflow valve for that respective train is inoperable. The RHR safety valves will provide overpressure protection of the RHR system.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/2 and 2/3 voting	Downstream voting logic becomes 1/2. No effects on the system level.	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	1/2 and 2/3 voting	Downstream voting logic becomes 2/2. No effects on the system level.	
35	LHSI Suction Isolation Valve	None	MHSI Large Miniflow Valves Interlock Between P14 and P17 Permissives	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid	Downstream voting logic modified to 2/2. No effects on the system level.	If a division is inoperable then the MHSI large miniflow valve for that respective train is inoperable. The RHR safety valves will provide overpressure protection of the RHR system.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/2 and 2/3 voting	Downstream voting logic becomes 1/2. No effects on the system level.	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	1/2 and 2/3 voting	Downstream voting logic becomes 2/2. No effects on the system level.	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS or Interlock	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
36	LHSI Hot Leg Injection Isolation Valve	None	MHSI Large Miniflow Valves Interlock Between P14 and P17 Permissives	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid	Downstream voting logic modified to 2/2. No effects on the system level.	If a division is inoperable then the MHSI large miniflow valve for that respective train is inoperable. The RHR safety valves will provide overpressure protection of the RHR system.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/2 and 2/3 voting	Downstream voting logic becomes 1/2. No effects on the system level.	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	1/2 and 2/3 voting	Downstream voting logic becomes 2/2. No effects on the system level.	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS or Interlock	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
37	APU	All	All	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting (For EDG actuation function: Redundant APU in same division)	All signals sent from affected APU marked invalid; Downstream voting logic modified (For EDG actuation, function is performed by redundant APU in same division)	Undetected - spurious failure of 1 APU can result in spurious EDG actuation Spurious failure of 1 APU and an APU out for maintenance (See Assumption Section) causes a spurious Turbine Trip. A spurious turbine trip is described in the safety analysis Section 15.2.2 (U.S. EPR FSAR Tier 2, Chapter 15). If a division is inoperable then the MHSI large miniflow valve for that respective train is inoperable. If an APU is inoperable the ability to detect the RHR connection for that division is lost. The RHR safety valves will provide the overpressure protection of the RHR system. The undetected-spurious failure of 1 APU will result in the spurious actuation of the MHSI large miniflow valves. This does not prevent the system from providing its safety function.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting (For EDG actuation, failure is in the safe direction)	Downstream voting logic becomes 1/2. (For EDG actuation, APU issues multiple spurious actuation signals.) (This condition causes a spurious Turbine Trip)	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	2/3 voting (For EDG actuation function: Redundant APU in same division)	Downstream voting logic becomes 2/2. (For EDG actuation, function is performed by redundant APU in same division)	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS or Interlock	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
38	Network APU - ALU	All	All	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting (For EDG actuation function: Redundant APU in same division)	All signals sent from affected APU marked invalid; Downstream voting logic modified (For EDG actuation, function is performed by redundant APU in same division)	Undetected - spurious failure of 1 APU can result in spurious EDG actuation. An inoperable APU results in a MCR Isolation and Filtering trigger. Spurious failure of 1 APU and an APU out for maintenance (See Assumption Section) causes a spurious Turbine Trip. A spurious turbine trip is described in the safety analysis Section 15.2.2 (U.S. EPR FSAR Tier 2, Chapter 16). If a division is inoperable then the MHSI large miniflow valve for that respective train is inoperable. If an APU is inoperable the ability to detect the RHR connection for that division is lost. The RHR safety valves will provide the overpressure protection of the RHR system.

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS or Interlock	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
39	ALU	All	All	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Redundant ALU in each subsystem. (For EDG actuation, redundant subsystem in same division)	ALU fails into state requesting RT, no ESF actuation; RT order generated in one division, RT devices voting logic becomes 1/3. One division unable to perform an ESF actuation. (For EDG actuation, redundant subsystem performs the function)	Undetected - spurious failure of 1 ALU can result in spurious ESF actuation (with the exception of EDG actuation). ESF Plant actuators which, if spuriously actuated can challenge plant safety require actuation orders from more than one division. For RCP trip function, failure of a functional unit such that all outputs are "1" is not postulated. This would be the failure of an output module. Therefore, the two RCP trip outputs from the same ALU (to two different RCP) must be through different output modules to prevent multiple spurious RCP trip. If a division is inoperable then the MHSI large miniflow valve for that respective train is inoperable. The RHR safety valves will provide the overpressure protection of the RHR system. The undetected-spurious failure of 1 ALU will result in the spurious actuation of the MHSI large miniflow valves. This does not prevent the system from providing its safety function.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	Redundant ALU in each subsystem; ESF spurious actuations in the safe direction	ALU fails into state requesting RT or EDG actuation, RT order generated in one division, RT devices voting logic becomes 1/3. For EDG actuation, redundant subsystem performs the EDG actuation. For ESF actuations, spurious actuation order is generated	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS or Interlock	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
40	Hardwired Output Logic	All	All	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	Three redundant divisions for RT; For ESF (including EDG actuation) failure is toward the safe state	Spurious RT order generated in one division. RT devices voting logic becomes 1/2; Spurious actuation of a single ESF actuator.	ESF plant actuators which, if spuriously actuated can challenge plant safety require actuation orders from more than one division.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant divisions for RT; Redundant divisions for ESF; Redundant hardwired logic within division for EFW isolation and EDG actuation.	One division unable to issue RT order, function performed by other 2 divisions; For ESF actuation, redundant divisions remain operable; For EDG actuation, affected subsystem unable to issue actuation, redundant subsystem in same division performs the function. For EFW isolation, redundant hardwired logic in same division performs the function	If a division is inoperable then the MHSI large miniflow valve for that respective train is inoperable. The RHR safety valves will provide the overpressure protection of the RHR system. The undetected-spurious failure of the hardwired output logic will result in the spurious actuation of a MHSI large miniflow valve. This does not prevent the system from providing its safety function.
41	Reactor Trip Device	All	None	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	Three redundant divisions of RT devices; 2/3 actuation.	Spurious RT order generated in one division. RT devices voting logic becomes 1/2	No effects on the system level.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant divisions of RT devices; 2/3 actuation.	One RT device fails to open; Remainder of RT devices function in 2/2 configuration.	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS or Interlock	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
42	PAC Module	None	All	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	Failure is toward the safe state.	Spurious actuation signal given to the attached actuator.	Plant actuators which, if spuriously actuated can challenge plant safety require actuation signals from more than one division to actuate (e.g., more than one pilot operator actuated from different divisions are required to change state of the main valve). If a division is inoperable then the MHSI large miniflow valve for that respective train is inoperable. The RHR safety valves will provide the overpressure protection of the RHR system. The undetected-spurious failure of the PAC module will result in the spurious actuation of a MHSI large miniflow valve. This does not prevent the system from providing its safety function. *For the RCP Trip function if a spurious PAC Module failure occurs, one RCP shall trip. This event is described in the safety analysis Section 15.3.1 (U.S. EPR FSAR Tier 2, Chapter 15).

ANP-10310NP – Methodology for 100% Combinatorial Testing of the U.S. EPR™ Priority Module Technical Report Markups

Glossary

Term	Definition
actuation signal	A signal received by the priority module device that requests initiation or termination of action of the final actuated device. There are three types of actuation input signal: latched, nonlatched, and delayed.
communication-priority pair	The term used to describe a PACS communication module and priority module pair. These modules are separate devices but are always paired to carry out the non-safety and safety functions, in support of the single actuated device they support.
delayed actuation signal	An actuation signal that must remain at a new valid logic value for a pre-defined period of time, before the new value is used in processing. For the special case of time-limited delay, the value used in processing can be different from the value of the input, following a transition from valid logic 0 to valid logic 1 and expiration of the time-limited delay. In this case, the value used in processing would be 0 and the input value could remain 1. *Note: This special case is anticipated to be used to control the overlapping test between protection system and priority module, ensuring that the test mode would be cancelled even in case of a permanently erroneously frozen input.*
infrastructure signal	A signal received by the priority module that indicates the status of elements that support the priority module (e.g., power supply status, output driver status, specific test modes). An infrastructure signal does not request an action of the final actuated device. It is used to set the output of the priority module to a predefined value, in case of a fault in an element supporting the priority module. Infrastructure signals are generated based only on signals originating in the module or the module's division.
latched actuation signal	A priority module input that functions as follows. Following an actuation input signal transition from a valid logic "1" to a valid logic "0", the logic "1" continues to be used in processing (i.e., it is latched). When a different (pre-designated) actuation input signal (e.g., an actuation signal in counter-direction) transitions from a valid logic "0" value to a valid logic "1", the latched value returns to a logic "0" for use in processing. This can be performed by a memory logic block with set/reset priority. (See Figure 7.1-1 in Tier 2 U.S. EPR™ FSAR.)
minimum stability time	The amount of time an input signal must remain stable at a priority module input terminal before it may be used in processing. The minimum stability time may be specific to individual signals, in accordance with the characteristics of the signal sources. The minimum stability time considers effects from synchronized sampling of inputs (all inputs from I&C and field signals pass through a D-flip-flop, to ensure stable inputs; this implies a delay between 0 and 1 clock cycle) and/or due to input debouncing which excludes short input spikes from processing. This implies a time delay, to manage the bouncing of limit switch contacts.

ANP-10315NP – U.S. EPR Surveillance Testing and TELEPERM XS Self-Monitoring Technical Report Markups

- APU function processor to the extent that the sensor measurement is acquired by the application software and the value used in the application software is viewed from the SAS service unit (SU).

The method used to perform a calibration depends on the type of sensor being tested. In cases where the sensor is accessible, and suitable test equipment exists (typical pressure, ~~and~~ level, speed, differential pressure, voltage and flow sensors), a substitute input to the sensor of the same nature as the monitored variable is used. The measurement value acquired by the application software in the function processor is viewed from the respective system's SU to verify accuracy of the measurement channel.

Calibration of resistance temperature detectors (RTDs) is performed by cross checks. During several isothermal plant conditions, the RTD values acquired in the APU or CU function processor application software can be viewed via the respective system's SU. The values of redundant RTD measurement are compared at each of the isothermal conditions to determine an acceptable value. Calibration parameters can then be adjusted in the application software so that each RTD measurement is accurate with respect to the cross calibrated value.

Calibration of analog rod cluster control assembly (RCCA) position measurements is performed by comparing it to the digital RCCA position measurements. The analog position measurement acquired by the application software in the APU function processor can be viewed from the PS SU. This value is compared with the digital RCCA position measurement provided by the reactor control surveillance and limitation system (RCSL~~S~~) to verify consistency within a specified tolerance.

Calibration of self-powered neutron detectors (SPND) is performed based on flux mapping by the aeroball measurement system (AMS). The principles of SPND calibration based on the AMS flux mapping are described in detail in Appendix B of ANP-10287P, "U.S. EPR Incore Trip Setpoint and Transient Methodology" (Reference

13). The resulting SPND calibration factors are entered into the APU function processor application software via the PS SU.

Calibration of boron concentration measurement is performed based on a reference measurement (e.g., chemical analysis of a sample of the fluid in the piping where the boron concentration measurement sensor is located). The boron concentration measurement acquired by the application software in the APU function processor can be viewed from the PS SU. This value is compared with the reference measurement to verify consistency within a specified tolerance.

Calibration of power range detectors is performed based on a power calorimetric and flux map performed at or above 20 percent reactor thermal power. The power range measurement acquired by the application software in the APU function processor can be viewed from the PS SU. The power range measurements are normalized based on the calorimetric and flux map results.

Calibration of intermediate range detectors is performed by obtaining the detector plateau or preamp discriminator curves, evaluating those curves, and comparing the curves with the manufacturer's data. The intermediate range measurement acquired by the application software in the APU function processor can be viewed from the PS SU and adjustments made based on results from comparing the curves with the manufacturer's data.

Calibration of the radiation monitors is performed based on a reference source of known radioactivity. The measurement value is viewed from the SICS and PICS to verify accuracy of the measurement channel. Calibration of the HMS is performed differently than the previously mentioned devices because the HMS does not interface with the PS or SAS. A substitute input to the sensor of the same nature as the monitored variable is used and the display of this variable is on the SICS and PICS. The measurement value is viewed from the SICS and PICS to verify accuracy of the measurement channel. For actuator position, the operator would place the actuator in the desired test position. The

measurement value is viewed from the SICS and PICS to verify accuracy of the measurement channel.

2.2.2 *Sensor Operational Test*

A sensor operational test is the injection of a simulated or actual signal into a PS or SAS division as close to the sensor as practicable, and capture of the injected signal when it reaches the application software of the APU or CU function processor. This process allows verification of accuracy and response time of devices between the sensor and the APU or CU function processor.

In the U.S. EPR PS design, sensor operational tests include the following equipment:

- Sensor signal path through any black-box monitoring systems.
- Sensor signal path through the signal conditioning and distribution system (SCDS).
- Input module of the APU.
- APU function processor to the extent that the sensor measurement is acquired by the application software and the value used in the application software is viewed from the PS SU.

In the U.S. EPR SAS design, sensor operational tests include the following equipment:

- Sensor signal path through any black-box monitoring systems.
- Sensor signal path through the signal conditioning and distribution system (SCDS).
- Input module of the CU.
- CU function processor to the extent that the sensor measurement is acquired by the application software and the value used in the application software is viewed from the SAS SU.

[

]

2.2.5.1 *ADOT for ~~ESFAS~~ Actuators Controlled by PS and SAS*

For ~~ESFAS~~ actuators controlled by PS and SAS, two overlapping tests (i.e., no-go test and go test) are used to provide test coverage of each component between the PS and SAS outputs and the actuator. In a no-go test, the PS and SAS activation signals are sent and acquired by the PACS priority module, but the outputs of the priority module are blocked to prevent the actuator from responding. In a go test, the non-safety-related I&C is used to exercise the actuator via the PACS priority module. The ADOT confirms both the functional capability and response time of the equipment between the PS outputs and the actuator. The ADOT confirms the functional capability of the equipment between the SAS outputs and the actuator.

2.2.5.1.1 ~~ESFAS~~ "No-Go" ADOT

Each ~~ESFAS~~ actuator controlled by PS and SAS has a dedicated PACS priority module. For a given ~~ESFAS~~ function, the PS or SAS sends actuation signals to the priority modules corresponding to the actuators required for that function. The no-go test duplicates this functionality by prompting the PS or SAS to send actuation outputs to all priority modules involved in a particular ~~ESFAS~~ function. Priority modules receiving

(e.g. RCP Trip) may be required only during outages. For manual controls that may be tested at power, one manual control is tested at a time. If a single manual control actuates a component, the checkback is displayed on the PICS. This is similar to the ESF "Go" ADOT except the actuation is initiated in SICS, and the checkback can be observed on PICS or SICS. If a single manual control does not actuate a device (e.g. 2-out-of-4 voting on 4 manual controls) the manual control's signal to the ALU can be read by the PS SU. When the manual control is input to the APU (e.g., boron concentration initialization), the SU must be connected to the APU to observe the result. The SAS has no technical specification surveillance requirements for manual controls.

Manual controls for permissive functions may be tested at power. One manual control can be initiated, when the conditions are not necessary for the permissive to change state. The manual control's signal to the APU can be read by the PS SU.

Manual component-level commands are generated in SICS and are connected directly to the PACS module for the actuated component. This test includes the conventional I&C in the SICS as well as the logic within the PACS module (e.g., Set/Reset memory logic block). The test is executed in SICS, and the checkback is displayed on the PICS.

2.2.6 *Channel Checks*

A channel check is defined in Technical Specifications. A channel check shall be the qualitative assessment, by observation, of channel behavior during operation. This determination shall include, where possible, comparison of the channel indication and status to other indications or status derived from independent instrumentation channels measuring the same parameter.

The automated channel check takes place in the gateway computer that interfaces the input signals in the PS and SAS to the Plant Data Network. The redundant signals from each division are compared periodically in the software to look for deviations between signals. In addition, the operator shall verify the performance of the automated channel check every 31 days.

Table 2-1—Software Based Self-Tests

Failures detected by inherent features - Failures that are detected by the self-test features as part of the system software (see Table 2-1 for the list of self-tests).

Failures undetected by inherent features - Failures that are not detected by the self-test features as part of the system software (e.g., a temporary fault of RAM cells that is repaired before it is detected by the self-test of the RAM).

Failures detected by engineered features - Failures that are detected by self-monitoring features designed as part of the application software (e.g., channel check or range monitoring).

Failures that are non-functional (failure does not prevent proper performance) - Failures that do not prevent the equipment from providing the proper execution of the function (e.g., a failure of the LED on the front plate of the module or a failure of the reset push button on the module). Since these types of failures are not required for the execution of the safety functions, it is not required to send these errors as alarms to the MCR.

Failures undetected by inherent features may be detected through engineered features.

If neither the inherent features or the engineered features detects the failure, then the failure is detected through periodic surveillance testing or is a non-functional failure.