U.S. EPR Design Features that Enhance Security

ANP-10296
Revision 2

Technical Report

June 2013

AREVA NP Inc.

Nature of Changes

Item Revision	Section(s) or Page(s)	Description and Justification
10.	All	Initial Issuance
21.	All	Changed document to Security Sensitive Information due to the inclusion of Aircraft Impact Assessment key design features and information.
31.	Sections 2.1, 2.2, 2.3, 2.4, 2.5, 2.8, 2.9, 2.12, 2.14, 2.15, 2.24, 2.27, 2.28, 2.29, 2.30, 2.31, 2.32, 2.33	Incorporate additional information to support U.S. EPR Design Certification Request for Additional Information (RAI) 565 and Aircraft Impact Assessment.
41.	All	Editorial changes including use of system acronyms.
2.		Corrected characterization of shock damage in some areas due to discrepancy in shock isolation gap discovered during drawing reviews.
2.		Corrected ATWS acronym.

Contents

List of Figures

Nomenclature

Acronym	Definition
AC	Alternating Current
AFW	Auxiliary Feedwater (See EFW)
AFWS	Auxiliary Feedwater System (See EFW)
ATWS	Anticipated Trip Transient Without SCRAM
CVCS	Chemical and Volume Control System
DC	Direct Current
DG	Diesel Generator
EBS	Extra Borating System
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EFW	Emergency Feedwater
ESFAS	Engineered Safety Feature Actuation System
ESW	Emergency Service Water
FPCS	Fuel Pool Cooling System
FSAR	Final Safety Analysis Report
I&C	Instrumentation and Controls
IRWST	In-Containment Refueling Water Storage Tank
LHSI	Low Head Safety Injection
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
MCC	Motor Control Center
MCR	Main Control Room
MHSI	Medium Head Safety Injection
PWR	Pressurized Water Reactor
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RPS	Reactor Protection System
RSB	Reactor Shield Building
RSS	Remote Shutdown Station
SAHRS	Severe Accident Heat Removal System
SBO	Station Blackout
SBODG	Station Blackout Diesel Generator
SFP	Spent Fuel Pool

Acronym	**Definition**
SI	Safety Injection
TMI	Three Mile Island
TNT	Trinitrotoluene (an explosive)
UL	Underwriters Laboratories

1.0 UTILIZATION OF CONCEPTS FROM NUREG/CR-1345

A majority of the general design concepts of NUREG/CR-1345, “Nuclear Power Plant Concepts for Sabotage Protection,” dated January 1981 (Reference 1) have been incorporated into the U.S. EPR design. The following tables review the topics and the degree of incorporation. Designation of NUREG/CR-1345 items is from Volume 2, Section D and Volume 2, Section E.

1.1 *Hardening Critical System/Locations*

ID	NUREG/CR-1345 Topic	U.S. EPR Design Feature
	HARDENING CRITICAL SYSTEM/LOCATIONS	
D3.2	Underground Site	Not Incorporated - Agreed with NUREG/CR-1345 Design Study Technical Support Group (1) too costly and (2) increased flood hazards. Also identified concern with replacement of large components. Hardened exterior structure is more cost effective and does not have flooding and equipment replacement concerns.
D3.3	Hardened Containment	Incorporated – See Section 2.1.
D3.4	Hardened Fuel Handling Building	Incorporated – See Section 2.2.
D3.5	Hardened Enclosure of Control Room	Incorporated – See Section 2.3.
D3.6	Hardened Enclosure for RPS and ESFAS Cabinets	Incorporated – See Section 2.4.
D3.7	Hardened Ultimate Heat Sink	Incorporated – See Section 2.10.
D3.8	Natural Protective Geographic Features	Site-Specific Feature. Addressed by Combined Operating License applicant.
D3.9	Hardened enclosure for Makeup Water tanks (Auxiliary Feedwater (AFW) Makeup)	Incorporated – See Section 2.6.

1.2 *Plant Layout Modification*

ID	NUREG/CR-1345 Topic	U.S. EPR Design Feature
	PLANT LAYOUT MODIFICATION	
D3.10	Separation of containment penetrations for redundant systems	Incorporated – See Section 2.9.
D3.11	Separation of piping, control cables, and power cables in underground galleries	Incorporated – See Section 2.11.
D3.12	Storage of Spent Fuel within Primary Containment	Not Incorporated - Spent fuel not stored within Containment but Fuel Building hardened against same external threats as containment. See Section 2.2.
D3.13	Spent Fuel Stored Below Grade	Not Incorporated - Spent fuel storage below grade is not feasible for U.S. EPR design due to reactor elevation. Additional redundant systems installed to enhance ability to cool spent fuel under adverse conditions. – See Sections 2.2, 2.14, and 2.15.
D3.14	Physically separate redundant trains of Safety Equipment	Incorporated - See Section 2.8.
D3.15	Separate Rooms for Cable Spreading	Incorporated - See Section 2.12.
D3.16	Alternate Control Room Arrangements	Incorporated - See Section 2.3 Hardened Shield over Main Control Room and 2.13 for diverse control systems.
D3.17	ECCS Components within Containment	Not Incorporated - Agreed with NUREG/CR-1345 Design Study Technical Support Group: (1) ECCS component containment access for surveillance and maintenance provides increased personnel risk; (2) utilization of diverse hardened Safeguard Buildings (See Sections 2.4 and 2.8) provides equivalent system protection. (NUREG/CR-1345 p. D-128).
D3.18	Information, Administration, and Construction Buildings located outside Protected Area.	Site-Specific Feature. Addressed by Combined Operating License applicant.

1.3 *System Design Changes*

ID	NUREG/CR-1345 Topic	U.S. EPR Design Feature
	SYSTEM DESIGN CHANGES	
D3.19	Isolation of Low Pressure System connected to RCS pressure boundary	Not Incorporated as stated – The U.S. EPR design utilizes additional check valves instead of additional isolation valves to reduce vulnerability to leakage outside containment. See Section 2.22.
D3.20	Design changes to facilitate Damage Control	Not Applicable – Four independent train design has minimized the need for damage control (cross-connecting) activities. Necessary cross-connections have been incorporated into the permanent design to minimize required operator actions.
D3.21	Alternate Containment Designs	Not Incorporated – The U.S. EPR design includes an advanced containment design (See Section 2.1) but does not include a filtered containment vent system.
D3.22	Extra redundant, fully separated, self-contained and protected trains of emergency equipment	Incorporated – See Section 2.8.
D3.23	Additional Protected Manual Control Rod Trip	Incorporated – See Section 2.24.
D3.24	Additional manually activated, diverse, protected Reactor Trip	Incorporated – See Section 2.24.
D3.25	Turbine Runback	Incorporated – See Section 2.19.
D3.26	Reduced vulnerability of intake structures for safety related pumps	Incorporated – See Section 2.20.
D3.27	Trip coils for breakers / Switchgear / Energized by Internal power source	Not Incorporated - insufficient benefit considering four vital busses each with dedicated diesel plus two Station Blackout Diesels. See Section 2.8.

D3.28	High Pressure RHR System	Partially incorporated - The U.S. EPR methodology accomplishes the same objective by providing 4 large capacity pumps that can inject to the RCS (4 MHSI pumps for U.S. EPR design vs. 2 SI and 2 High Pressure RHR as proposed for previous designs). The U.S. EPR operating philosophy is to rapidly reduce pressure to the point where the MHSI system can inject. Lower RCS pressure both allows injection of 4 trains of independent MHSI System and reduces the impact of any leakage by reducing the driving force.

1.4 *Additional Systems*

ID	NUREG/CR-1345 Topic	U.S. EPR Design Feature
	ADDITIONAL SYSTEMS	
D3.29	Hardened Decay Heat Removal System (All Steam Powered Version)	Not Incorporated - Steam driven equipment is less reliable than motor driven equipment. Redundant electrically driven equipment used preferentially. See Sections 2.5 and 2.6.
D3.30	Independent diverse SCRAM systems.	Incorporated – See Section 2.24.

1.5 *Generic Design Changes*

ID	NUREG/CR-1345 Topic	U.S. EPR Design Feature
	COMPONENT DESIGN CHANGES	
E2.1	AC Power System Swing-Load Capability	Incorporated - Divisions 1 and 4 have dual feed capability (Normal Emergency Diesel Generator and a Station Blackout Diesel). Divisions 2 and 4 can be fed by Emergency Diesel Generator and by manual alignment from Divisions 1 and 4.
E2.2	Switchgear and MCC Enclosure Internal Circuit Breaker Trip Capability	Not Incorporated – with four redundant trains, the tripping of one train has little or no safety impact especially when that would not preclude operator action to re-close the breaker upon discovery. See Section 2.8.
E2.3	Vital Electrical Area Revised Cooling Arrangements	Incorporated – See Section 2.10.
E2.4	Multiple Unit Vital AC Cross-Connections	Not Applicable - The base design is a single unit.

ID	NUREG/CR-1345 Topic	U.S. EPR Design Feature
	COMPONENT DESIGN CHANGES	
E2.5	Diesel Engine Revised Cooling Arrangements	Incorporated on SBODGs – See Section 2.16.
E2.6	Increased Protected Diesel Fuel Oil Supply	Incorporated – See Section 2.17.
E2.7	Revised Diesel Building Layout (Thermal Habitability)	Partially Incorporated- Diesel controls are in a separate room from diesel generator to enhance accessibility but that room not on a separate ventilation system. There is little value to providing separate systems since adversary access to the building to damage main ventilation also provides access to damage controls. Redundancy and spatial separation already in the design substantially increases difficulty of damaging all diesel generators.
E2.8	Increased Vital battery Capacity (from 2-4 hrs to 6-8 hrs)	Not Incorporated - insufficient benefit considering battery chargers on each of four vital busses each with dedicated diesel plus two SBODGs.
E2.9	DC Load Shedding Capability	Not Applicable - Site-Specific Operating Procedures Feature. Addressed by Combined Operating License applicant.
E2.10	Class 1E DC Division Cross-Connections	Not Incorporated - insufficient benefit considering battery chargers on each of four vital busses each with dedicated diesel plus two SBODGs.
E2.11	Extended DC power Generation Capability during Station Blackout	Incorporated concept of multiple diesels each capable of providing DC power capabilities - See Section 2.8.
E2.12	Consolidation of Safety Related Instrumentation Transmitters	Not Incorporated – Instead of consolidated equipment in one location, the U.S. EPR design has spatially separated components to minimize common risks to multiple divisions of equipment. See Section 2.12 and 2.13.
E2.13	Additional Local-Remote Indicators	Not Incorporated – General “walk-downs” and rounds by operations personnel are beneficial for detections of abnormal conditions. Elimination of these in favor of remote indications would be a detriment to the overall surveillance of the equipment and detection of tampering.
E2.14	Rearrangement of Instrument Cabinet Panel-Front Devices (minimize opening cabinets)	Not Incorporated – This feature is a characteristic of the detailed design of the components.

ID	NUREG/CR-1345 Topic	U.S. EPR Design Feature
	COMPONENT DESIGN CHANGES	
E2.15	Small-Diameter Piping Modifications (thicker, all-welded pipe <1”)	Incorporated - The U.S. EPR design uses all welded pipe for the RCS Pressure Boundary.
E2.16	Component Passive Lubrication (minimize pressurized oil systems)	Incorporated – The U.S. EPR safe-shutdown related systems, other than the Diesel Generators, do not utilize a pressurized oil system for lubrication of critical components.
E2.17	Modular Components (use of sealed inaccessible parts for reduction of tampering)	Partially Incorporated – Modular components have been used where prudent to streamline maintenance and construction.
E2.18	Component Cooling Modifications	Not Included – The components of the various trains are already cooled via diverse methods. Two trains are cooled directly with external cooling water and two trains are cooled via internal air-cooled systems which are secured entirely within the Safeguard Building it supports. See Section 2.10.
E2.19	Vital Area Emergency Cooling Modifications	Not Included – The components of the various trains are already cooled via diverse methods. Two trains are cooled directly with external cooling water and two trains are cooled via internal air-cooled systems which are secured entirely within the Safeguard Building it supports. See Section 2.10.

1.6 *PWR Design Changes*

ID	NUREG/CR-1345 Topic	U.S. EPR Design Feature
	DAMAGE CONTROL MEASURES	
E3.1	Class 1E Auxiliary Steam Turbine Generator	Not Incorporated - Turbine driven equipment is generally more unreliable than motor driven equipment. Multiple trains with dedicated diesel units were deemed to be inherently more reliable. EDGs 1&2 are an alternate-feed pair via maintenance connections, EDGs 3&4 are an alternate-feed pair via maintenance connections, and the SBODGs can be connected to either Bus 1 or 4. Incorporation of four EDG divisions and two SBODG divisions (6 independent sources) adds additional level of diversity to reduce vulnerability. See Section 2.8.

ID	NUREG/CR-1345 Topic	U.S. EPR Design Feature
	DAMAGE CONTROL MEASURES	
E3.2	Class 1E Pressurizer Heater power (assurance of subcooling)	Partially Incorporated – The U.S. EPR design includes Class 1E Power for the Pressurizer heater in accordance with the TMI Action Plan item. The allowable cooldown rate and insulation requirements were evaluated for LOOP conditions. The U.S. EPR design can maintain nominal operational pressure (Hot Standby) during LOOP for 2 Hours after reactor trip assuming single failure in one Emergency Diesel Generator.
E3.3	Additional Pressurizer Insulation (reduces Pressurizer cooldown therefore reduced loss of subcooling)	Partially Incorporated - The allowable cooldown rate and insulation requirements were evaluated. The U.S. EPR design can maintain nominal operational pressure (Hot Standby) during LOOP for 2 Hours after reactor trip assuming single failure in one Emergency Diesel Generator.
E3.4	Reactor Vessel Water Level Instrumentation	Incorporated – See Section 2.23.
E3.5	Reactor Vessel Head Vent	Incorporated – The U.S. EPR design has a high point vent system.
E3.6	RCP seal controlled leak-off isolation valve actuator	Incorporated variation – See Section 2.18.
E3.7	Parallel Auxiliary Spray Valves	Incorporated – See Section 2.26.
E3.8	Automatic AFW Actuation	Incorporated – See Section 2.21.
E3.9	Increased Emergency Feedwater Supply	Incorporated variation – See Section 2.6.
E3.10	AFWS Motor-Driven pump Swing-Load Capability	Incorporated variation – See Section 2.8.
E3.11	Additional Local AFWS Instrumentation (for local Turbine control)	The U.S. EPR design does not utilize Turbine-Driven equipment.
E3.12	DC Powered Turbine/Pump Auxiliaries	The U.S. EPR design does not utilize Turbine-Driven equipment.
E3.13	Elimination of AFW Turbine Pump Room Steam Leakage	The U.S. EPR design does not utilize Turbine-Driven equipment.
E3.14	Relocation of Turbine Driven AFW subsystem Local Instrumentation and controls	The U.S. EPR design does not utilize Turbine-Driven equipment.
E3.15	AFW Turbine Pump Room Ventilation System Modification	The U.S. EPR design does not utilize Turbine-Driven equipment.

ID	NUREG/CR-1345 Topic	U.S. EPR Design Feature
	DAMAGE CONTROL MEASURES	
E3.16	Increased ECCS Safety Injection Tank Pressure (larger Boron Injection Tank and/or accumulators)	There are redundant Extra Borating System Pumps/Tanks having a minimum required available total volume of approximately 1994ft^3 (14,920 gal). This is much larger than the single 900 gallon Boron Injection Tank utilized by the previous generation of reactors on which this recommendation was based.
E3.17	Reduced Loss of Coolant Accident (LOCA) potential in Pressurized Water Reactor (PWR) RHR System	Not Incorporated – See Item D3.17 above - Agreed with NUREG/CR-1345 Design Study Technical Support Group: (1) ECCS component containment access for surveillance and maintenance provides increased personnel risk; (2) utilization of diverse hardened Safeguard Buildings provides equivalent system protection. The U.S. EPR operating philosophy is to rapidly reduce pressure to the point where the MHSI system can inject. Lower RCS pressure both allows injection of 4 trains of independent MHSI System and reduces the impact of any leakage by reducing the driving force.

2.0 DESCRIPTION OF DESIGN ELEMENTS THAT ENHANCE SECURITY

The U.S. EPR design relies upon the incorporation of proven technologies and reliability standards manifested in system redundancy, diversity, and independence. This safety philosophy is based on deterministic consideration of defense-in-depth complemented by probabilistic analyses that were developed from European deployment and enhancements identified in the U.S. EPR development effort.

2.1 *Hardened Shield Building Over Containment*

The Shield Building (Figure 2-1), which encases the Containment, is a reinforced concrete structure designed to provide protection against external hazards, including a direct impact from a large commercial aircraft. The walls of the Reactor Shield Building (RSB) are thicker than typically found in previous reactor designs and sufficiently robust to prevent penetration of the structure. The external shield wall is designed so that during a commercial aircraft impact the external shield wall will not impact the internal structure, thus providing shock isolation. The shield structure is shock isolated from the containment structure to require shock to travel to the base mat before affecting the equipment located in containment. No safety-related system piping is attached directly to the shield structure walls.

The RSB protects equipment inside containment (e.g., main feedwater, main steam, steam generator, reactor coolant system (RCS), control rod drive mechanisms, etc.) against substantial damage generally associated with physical impacts damage or shock damage from the impact.

The structure also protects personnel and equipment against other substantial damage generally associated with the resulting fire or smoke from the impact.

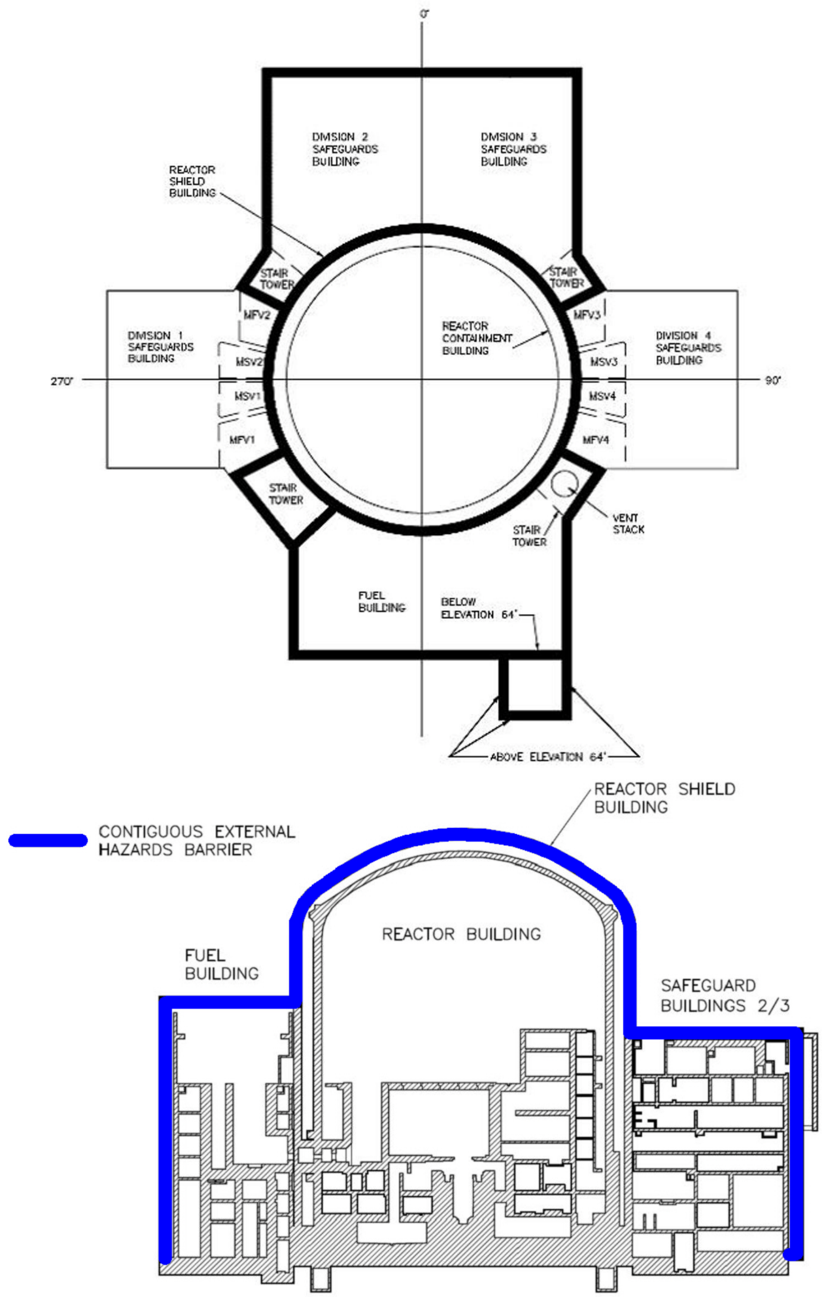
For additional information, refer to AREVA NP Technical Report ANP-10317 and U.S. EPR FSAR Tier 2, Sections 1.2.3.1.2 and 3.8.

2.2 *Hardened Shield Building Over Fuel Building*

The buttressed Shield Building (Figure 2-1), which covers the Fuel Building, is a reinforced concrete structure designed to provide protection against external hazards, including a direct impact from a large commercial aircraft. The walls of the Shield Building are sufficiently robust to prevent perforation of the structure. The shield structure is shock isolated from the Fuel Building structure to require shock to travel extended distancesto the base mat before affecting the equipment located in the Fuel Building. The external shield wall is designed so that during a commercial aircraft impact the external shield wall will not impact the internal structure, thus providing shock isolation. No safety-related system piping is attached directly to the shield structure walls. The structure also protects personnel and equipment against other substantial damage generally associated with the resulting fire or smoke from the impact.

For additional information, refer to U.S. EPR FSAR Tier 2, Section 1.2.3.1.2.

Figure 2-1—Robust Shield Building



2.3 *Hardened Shield Building Over Safeguard Buildings 2 and 3*

A buttressed Shield Building encases Safeguard Buildings 2 and 3 where the main control room (MCR) and remote shutdown station (RSS) are housed (Figure 2-1). This reinforced concrete structure is designed to provide protection against external hazards, including a direct impact from a large commercial aircraft. The external shield wall is designed so that during a commercial aircraft impact the external shield wall will not impact the internal structure, thus providing shock isolation. The shield structure is shock isolated from the containment structure to require shock to travel to the base mat before affecting the equipment located in containment. No safety-related system piping is attached directly to the shield structure walls. The walls of the Shield Building are sufficiently robust to prevent penetration of the structure. This protects personnel and equipment against impact, fire, and smoke damage generally associated with the impact.

For additional information, refer to U.S. EPR FSAR Tier 2, Sections 1.2.3.1.2 and 3.1.2.10.1.

2.4 *Hardened Shield Building over ECCS Components*

A buttressed Shield Building (Figure 2-1) encases structures containing two of the four trains of emergency core cooling system (ECCS) equipment. No safety-related system piping is attached directly to the shield structure walls. The two other trains are in diversely located structures so that one event cannot affect both structures and have external walls that are sufficiently robust to prevent penetration of the structure. These reinforced concrete structures and diverse locations are designed to provide significant protection against external hazards, including a direct impact from a large commercial aircraft.

For additional information, refer to U.S. EPR FSAR Tier 2, Sections 1.2.3.1.2 and 3.5.1.6.

2.5 *Hardened Decay Heat Removal Systems*

The emergency service water (ESW) cooling tower and pump structures are specific to one low head safety injection (LHSI) and residual heat removal (RHR) train and are physically diverse such that one event cannot disable more than two trains. The ESW structures are situated such that the cooling towers supporting Safeguard Buildings 2 and 3 (i.e., the trains under the robust shielding) are placed on opposite sides of the Nuclear Island and are placed to the interior (closer to the Nuclear Island) as to be partially shielded by the remaining trains.

Each train of emergency feedwater (EFW) and its associated ESW division is independently capable of removing post-trip decay heat and stabilizing the unit at Hot Shutdown conditions (<350°F).

The division 1 and 2 ESW pump and cooling tower structures are separated from the division 3 and 4 ESW pump and cooling tower structures by the shield structure covering Safeguard Buildings 2 and 3, the RSB, and the Fuel Building. Divisions 1 and 2 ESW structures are also separated from Divisions 3 and 4 ESW structures by at least 300 feet. These structures are not simultaneously affected by a single aircraft strike event. At least two ESW pumps and towers will not be affected by the aircraft impact event.

For additional information, refer to U.S. EPR FSAR Tier 2, Sections 1.2.3.1.2, 3.5.1.6, 9.2.1, 9.2.2, and 9.2.5.

2.6 *Hardened and Internalized Emergency Feedwater Tanks*

A robust Shield Building encases structures containing two of the four trains of EFW equipment. The two other trains are in diversely located structures so that one event cannot affect both structures. These reinforced concrete structures and diverse locations are designed to provide significant protection against external hazards, including a direct impact from a large commercial aircraft. Use of four independent EFW systems each with an excess of 6 hours of decay heat removal capability produces at least 24 hours of operation (assuming system rotation or utilization of cross-connections) before makeup is required.

For additional information, refer to U.S. EPR FSAR Tier 2, Sections 1.2.3.1.2, 3.5.1.6, and 10.4.9.

2.7 *Hardened and Internalized Emergency Core Cooling Water*

The in-containment refueling water storage tank (IRWST) maintains a large reserve of borated water at a homogeneous concentration and temperature. The borated water is used during refueling to flood the refueling cavity and is also the safety-related source of water for LHSI/RHR containment cooling, ECCS injection, and severe accident heat removal system (SAHRS) cooling.

The emergency core cooling water supply is located within containment; therefore, it is protected by the Shield Building. Having the supply inside containment limits the adversarial actions that could impact the availability of this injection source. The protection afforded to personnel and equipment from aircraft threat provides increased assurance that supporting personnel and equipment are available to take the necessary actions following the event.

For additional information, refer to U.S. EPR FSAR Tier 2, Section 1.2.3.1.2, 3.5.1.6, and 6.3.

2.8 *Physically Separate and Redundant Trains*

Each of the four ECCS trains is housed in a separate physically isolated hardened structure. Each of the four ECCS electrical buses are housed in a separate physically isolated hardened structure and two trains are in shock protected portions of the structures that limit shock damage. A dedicated Emergency diesel generator (EDG) is available for each of the four trains and two station blackout (SBO) diesel generators (SBODG) are capable of supplying multiple trains. This design provides high assurance that required systems have power when required. EDGs 1 and 2 are alternate-feed pairs, EDGs 3 and 4 are alternate-feed pairs, and the SBODGs can be connected to Divisions 1 or 4. Incorporation of four EDG divisions and two SBO divisions (6 independent sources) adds an additional level of diversity to reduce vulnerability. Multiple divisions, reinforced concrete structures with robust external doors, and spatial separation of trains are design elements intended to provide significant protection against external hazards and hostile actions.

The Emergency Power Generating Building (EPGB) structures are separated by the Safeguard Buildings 2 and 3 shield structure. These structures (each housing two EDGs) are at least 300 feet apart and therefore are not simultaneously affected by a single aircraft strike event. At least one EPGB (housing two EDGs) will not be affected by the aircraft impact event.

For additional information, refer to U.S. EPR FSAR Tier 2, Sections 1.2.3.1.1 and 1.2.1.

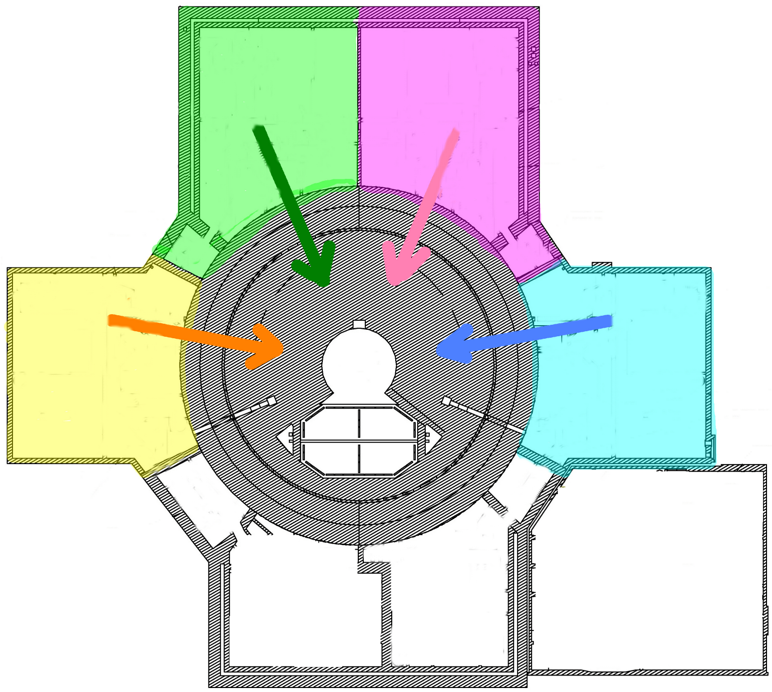
2.9 *Containment Penetrations*

The four equipment trains are routed through a series of containment penetrations directly from the specific Safeguard Building through the annulus into containment (Figure 2-2). Cables, piping, and control circuits from one train are spatially and physically separated from other trains. This train separation provides an added assurance that a single event does not impact multiple trains and adds substantial difficulty to adversarial actions attempting to disable equipment. Accesses to the penetrations are solely from areas already heavily protected.

The Containment pressure sensing line CIVs are 0.5” manually operated valves that are normally open. These CIVs are located in SGB2, SGB3, and the Fuel Building, which are shielded buildings.

For additional information, refer to U.S. EPR FSAR Tier 2, Sections 3.4.3.3 and 6.3.1.

Figure 2-2—Piping Routes to Containment



2.10 *Safeguard Building Cooling Systems*

Each of the four Safeguard Buildings is a separate structure with separate cooling systems. Two of the four Safeguard Buildings are ultimately cooled by the ESW cooling towers, which serve as the ultimate heat sinks, and two trains are ultimately cooled by an air-cooled train of the safety chilled water system contained entirely within that significantly hardened structure. A dedicated EDG for each of the four divisions and two SBODGs, which are capable of supplying multiple trains, provide high assurance that required systems have power when required. Multiple trains, reinforced concrete structures with robust external doors, and spatial separation of trains are design elements intended to provide significant protection against external hazards and hostile action.

For additional information, refer to U.S. EPR FSAR Tier 2, Sections 9.4.5 and 9.2.8.

2.11 *Safety-Related Underground Piping and Cables*

The four ECCS train electrical cables are routed through separate isolated cable pathways to the train or division specific electrical bus. This train separation provides an added assurance that a single event does not impact multiple trains.

2.12 *Cable Spreading and Associated Cable Routing Issues*

Each of the four ECCS train or division electrical and control cables are routed through separated pathways to the MCR and the RSS. Redundant cable spreading areas are used to minimize the impact of damage to either area. Reinforced concrete structures and spatial separation of trains are design elements intended to provide significant protection against external hazards and hostile actions.

Electrical isolation is required for hardwired and data connections, and is provided through the use of qualified isolation devices and fiber optic cable.

For additional information, refer to U.S. EPR FSAR Tier 2, Section 9.5.1.2.1.

2.13 *Distributed Digital Control Systems*

U.S. EPR instruments and controls (I&C) systems and equipment are redundant, spatially separated, and diversified. For example, the safety injection system and the EFW system each consists of four redundant and independent trains (one in each of the four Safeguard Buildings) and has four redundant and independent I&C channels (one in each of the four Safeguard Buildings). Each safety-related I&C system is designed to fulfill its functions even if one of the channels is not available because of a failure and at the same time, another of its channels is not available for preventive maintenance or because of an internal hazard (e.g., fire). The logic utilizes a majority voting whether the voting is between 4 divisions (2 of 4 logic), three divisions (2 of 3 logic), or two divisions (1 of 2 logic). The failure of the automatic system to actuate does not prevent manual action by operators.

For additional information, refer to U.S. EPR FSAR Tier 2, Section 7.8.

2.14 *Spent Fuel Cooling and Makeup Systems*

Each of the two fuel pool cooling system (FPCS) trains is located in isolated areas of the Fuel Building. Damage to either of the two isolated areas will not disable the other train, reinforced concrete structures with robust external doors, and spatial separation of trains are design elements intended to provide significant protection against external hazards, and to add substantial difficulty to adversarial actions attempting to disable the Spent Fuel Pool (SFP) cooling functions.

The normal SFP Makeup is provided by the fuel pool cooling and purification system (FPCPS) as described in U.S. EPR FSAR Tier 2, Section 9.1.3.2.4. Additional makeup capability is provided by beyond design basis systems located in the stairwells on opposite sides of the refuel floor which utilize embedded pipe to the SFP. These systems are designed to recover leakage from the lower levels of the Fuel Building, be supplied by the fire protection system, or be supplied by external connections to independently powered portable pumps.

Depending on the time since last refueling, the SFP will require 4 hours or more to begin boiling. After boiling has begun, it takes at least 25 hours until the fuel is exposed, providing sufficient time to initiate SFP makeup mitigating actions.

Instrumentation is provided to monitor the pool water level and water temperature to provide indication of the loss of water and degradation of the decay heat capability. Instrumentation is located outside the shock damage footprint.

For additional information, refer to U.S. EPR FSAR Tier 2, Section 9.1.3.

2.15 *Spent Fuel Pool Spray and Makeup Systems*

A SFP Spray System is included in the Fuel Building to recover any substantial leakage from the SFP should damage occur. This system recovers the leakage from the lower level of the Fuel Building and sprays it back into the SFP to minimize the risk of damage to fuel.

SFP spray capability is provided by beyond design basis systems located in the stairwells on opposite sides of the refuel floor which utilize embedded pipe to the SFP spray header. These systems are designed to recover leakage from the lower levels of the Fuel Building, be supplied by the fire protection system, or be supplied by external connections to independently powered portable pumps.

SFP cooling may be accomplished by providing makeup water to the SFP from a source external to the SFP floor and allowing the SFP to boil. The makeup source is AC independent and therefore has no dependencies on installed SFP cooling system cooling or power equipment. Redundant SFP fill systems to support long term refill operations without requiring access to the SFP area are installed in the Fuel Building and are protected from damage by the Fuel Building Shield structure. Redundant valves are located in the stairways **[ ]**.

2.16 *Air Cooled Diesels*

The design incorporates two SBODGs, which are independent of external cooling water and instead use a forced-draft radiator for diesel heat rejection. The SBODG System is coupled with area cooling in Safeguard Buildings 1 and 4 that do not rely on external cooling water. Together, these two systems are capable of supporting equipment necessary to reach and maintain stable conditions without use of external cooling water. Forced-draft radiator diesel cooling system is presently in use at several nuclear power plants.

For additional information, refer to U.S. EPR FSAR Tier 2, Section 8.4.

2.17 *Diesel Fuel Oil Storage Protection*

Each of the four EDG has a dedicated diesel fuel oil tank enclosed within the Emergency Power Generating Building. Access to the diesel fuel oil tank is internal to the Emergency Power Generating Building. This arrangement provides:

1. Four spatially separated fully independent tanks.

2. Hardened protective enclosure for each tank.

3. Restricted access to each tank.

Each of the two Station SBODG has a dedicated diesel fuel oil tank. Access to the diesel fuel oil tank is from within the hardened structure containing the SBODG. This arrangement provides:

1. Two spatially separated fully independent tank.

2. Hardened protective enclosure for each tank.

3. Restricted access to each tank.

For additional information, refer to U.S. EPR FSAR Tier 2, Section 9.5.4.

2.18 *Improved Reactor Coolant Pump Seals*

The U.S. EPR design utilizes a “standstill” seal that provides redundancy so that a failure of a single seal stage does not result in an uncontrolled loss of reactor coolant. The reactor coolant pumps (RCPs) use a mechanical shaft seal system that consists of three seals arranged in series with a standstill seal. The first seal is a controlled leakage, film-riding face seal; the second and third seals are rubbing-face seals. The standstill seal is a metal-to-metal contact seal that prevents leakage when the RCP has stopped and the three seal leak off lines have been isolated. The standstill seal is normally used under the following conditions:

- In the event of a concurrent loss of injection water (chemical and volume control system, CVCS) and cooling water for the thermal barrier (component cooling water system, CCWS).
- In the event of concurrent failure of all three shaft seals.

The standstill seal is activated by compressed nitrogen and is designed to stay closed if the gas pressure is lost, and to remain closed and maintain RCS pressure boundary integrity down to an RCS pressure of approximately 218 psia. If the nitrogen pressure is maintained on the standstill seal, it will maintain RCS pressure boundary integrity down to zero RCS pressure. Position indication is provided for the standstill seal. Standstill seal operability is maintained after a safe shutdown earthquake (SSE).

For additional information, refer to U.S. EPR FSAR Tier 2, Section 1.2.3.2.6.

2.19 *Loss of Offsite Power and Turbine Runback*

In the event of loss of offsite power, the plant will accept a generator load rejection of 100 percent power or less without reactor trip, and be able to continue stable operation with minimum auxiliary loads (i.e., house loads). With this feature, the low-power reactor operation continues to provide site equipment requisite power until offsite power is again available.

Should the reactor trip for other reasons, the U.S. EPR design also includes four safety-related diesel generators each capable of providing 100 percent of the power required to reach and maintain safe shutdown. Each diesel is associated with an independent train. In addition to these four EDGs, the U.S. EPR design has two SBODGs with diverse connectivity to provide additional assurance that required systems have the requisite power.

For additional information, refer to U.S. EPR FSAR Tier 2, Table 19.1-2.

2.20 *Reduced Vulnerability of Intake Structures*

The U.S. EPR design is equipped with four dedicated independent ESW system trains that serve as the ultimate heat sink to transfer decay heat generated by the core and the SFP to the atmosphere. The ESW system is located in four hardened structures which collectively contain approximately 10 million gallons of water entirely within the site Protected Area.

Each ESW system train maintains sufficient water mass to conservatively provide cooling for three days following reactor trip without makeup from external intake structures. This reduces the reliance on cooling water make-up intake structures for safe shutdown. Decay heat is a function of time since shutdown and substantially reduces over the first three day period. Using estimates of the heat generated by the minimum electrical loads required to maintain hot standby, the SFP cooling load and the RHR system heat loads, it is estimated that sufficient water exists onsite in the ESW basins for 15-30 days depending on time since last refueling outage.

Additional action by the Emergency Response Organization during the first 15 days following the event provides for replenishing of the water in the ESW basins to support extended operation if required.

For additional information, refer to U.S. EPR FSAR Tier 2, Section 9.2.5.

2.21 *Minimal Reliance on Operator Immediate Actions*

The design of the U.S. EPR systems, structures, and components, including control and protection systems, minimizes operator actions required to mitigate design basis accidents or anticipated operational occurrences within the following constraints:

- No operator action prior to 30 minutes if taken from the MCR.
- No operator action prior to 60 minutes if performed outside the MCR.

This includes automatic initiation of EFW and RCS injection to provide adequate core protection.

This minimizes operator movement necessary during security events. Minimizing movement by plant staff during assaults will enhance the security staff’s ability to detect movement of adversaries. This also reduces the critical communications between the two departments during this high activity timeframe; reducing the potential for critical errors due to miscommunications.

For additional information, refer to U.S. EPR FSAR Tier 2, Sections 15.0.0.3.7, 1.2.1, 6.2.1.4.1.3, and 6.3.2.8.

2.22 *Improved Pipe Rupture Backflow Protection*

Where previous generation designs had one check valve in containment to prevent high pressure RCS leakage into connecting systems, the U.S. EPR design has at least two check valves or two isolation valves on each line with direct RCS connection. This provides an increased level of protection against failure of a check valve resulting in RCS leakage outside containment.

2.23 *Reactor Vessel Level Indicating System*

The reactor vessel is provided a Class 1E level monitoring system that remains operable during design basis accident conditions and provides internal water levels.

For additional information, refer to U.S. EPR FSAR Tier 2,Table 7.5-1.

2.24 *Anticipated Transient without SCRAM Mitigation*

The U.S. EPR design utilizes a Diverse Actuation System (DAS) to mitigate the consequences of anticipated transient without SCRAM (ATWS). This system provides multiple diverse signals for the control rods to insert. Accordingly, the probability of having a common cause failure that causes 50 percent or more of the control rods to fail to insert is extremely small and is not a significant contributor to the probability of an ATWS. The ability to open the reactor trip breakers and allow gravity to cause the control rods to insert is protected by the placement location of the reactor trip breakers in shock protected areas **[ ]**.

Additionally, the extra borating system (EBS) is available as a manually operated redundant reactivity control systems. The EBS system components lay outside the shock damage footprint with the exception of instrumentation that provides indications only and that will not prevent the EBS system from operating.

For additional information, refer to U.S. EPR FSAR Tier 2, Section 7.8.

2.25 *Molten Core Retention and Cooling*

The U.S. EPR design is equipped with a dedicated system to retain and cool the molten core debris that can penetrate the reactor pressure vessel up to and including the entire core inventory, reactor internals, and residual portions of the lower vessel head. The system stabilizes molten core debris prior to it challenging the integrity of containment. The reactor cavity utilizes a combination of sacrificial concrete and refractory layer to provide a stage of temporary melt retention. Once the molten core is within the spreading compartment, the water from the IRWST will start to passively fill the cooling structure. This flooding is expected to result in submergence of the spreading area, thereby stabilizing the core debris in those areas.

Operating in the passive mode, IRWST water, supplied by the SAHRS System, will be boiled off as steam and released into the containment, which is capable of handling several hours of passive operations with no containment cooling. SAHRS supporting systems will ultimately transfer the heat from containment to the ESW cooling tower, which is the ultimate heat sink.

This retention of core debris in an undamaged containment, even during the worst of accident conditions, greatly reduces the impact to the public of any adversary action.

For additional information, refer to U.S. EPR FSAR Tier 2, Section 1.2.3.3.4.

2.26 *Redundant Auxiliary Spray Valves*

The U.S. EPR design utilizes three independent pressurizer spray trains. Two normal spray trains provide spray from coolant loops 2 and 3 while one auxiliary spray provides spray from the CVCS. The trains are diverse in that each spray train is powered by a separate emergency power train (loop 2 from division 2, loop 3 from division 3, and auxiliary spray from division 4). In addition, depressurization of the RCS during emergency conditions will be conducted utilizing an emergency depressurization system to reduce pressure to the point that the medium head safety injection can inject. This additional pressure control system reduces the reliance on pressurizer sprays.

For additional information, refer to U.S. EPR FSAR Tier 2, Sections 1.2.3.2.4 and 5.4.10.2.1.

2.27 *Cask Loading System and Penetrations*

The cask loading system connection is below the SFP normal water level. This method is used in some European reactors but is uncommon in U.S. reactors. Key design features of the cask loading system are listed in U.S. EPR FSAR Tier 2, Section 19.2.7.4.

2.28 *Main Steam and Main Feedwater Line Impact Protection*

[

]

2.29 *MSRT Exhaust Protection*

[

]

2.30 *Protection of Cross Tied Systems*

[

]

[

]

Electrical connections are protected by faults in the alternate pair division by breakers.

Equalizing piping between the secondary side of the Steam Generators is located inside Containment and is protected from physical, fire, or shock damage.

2.31 *AIA Structures of Concern*

[ ]

2.32 *AIA Programmatic Assumptions*

[ ]

2.33 *AIA Analysis Assumptions*

3.0 REFERENCES

1. NUREG/CR-1345, “Nuclear Power Plant Concepts for Sabotage Protection,” January 1981.

2. NEI 07-13 Revision 8, “Methodology for Performing Aircraft Impact Assessment for New Plant Designs”, April 2011.

3. ANP-10295NP Revision 4, “U.S. EPR Security Design Features Technical Report,” April 2013.

4. ANP-10317 Revision 1, “Design Requirements for the U.S. EPR Aircraft Hazard Protection Structures,” April 2013.