Response to

Request for Additional Information No. 2, Revision 0

4/10/2008
U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 19 - Probabilistic Risk Assessment and Severe Accident Evaluation
Application Section: 19
SPLA Branch

Question 19-01:

Section 19.0.1, “NRC Regulatory Requirements and Related Policies,” does not include several items listed in Section 19.0 of the Standard Review Plan (SRP). For completeness, please confirm in Section 19.0.1 that the following requirements and guidance either were considered or are not applicable: (1) Title 10 of the Code of Federal Regulations (10 CFR) 52.47(a)(8); (2) 10 CFR 52.47(a)(23); (3) 10 CFR 52.47(a)(27); (4) NRC Policy Statement, “Regulation of Advanced Nuclear Plants”; (5) SECY-96-128 and the related Staff Requirements Memorandum (SRM); (6) SECY 97-044 and the related SRM.

Response to Question 19-01:

A response to this question will be provided by May 30, 2008.

Question 19-02:

Footnote 8 in RG 1.206, Section C.I.19, Appendix A, states that: "'PRA [probabilistic risk assessment]-based insights' are those insights identified during the DC [design certification] process that ensure that assumptions made in the PRA will remain valid in the as-to-be-built, as-to-be-operated plant and include assumptions regarding SSC [structure, system, and component] and operator performance and reliability, ITAAC [inspections, tests, analyses, and acceptance criteria], interface requirements, plant features, design and operational programs, and others. The usage of the phrase is intended to be consistent with its use in Table 19.59-29 of the AP600 design control document [DCD]." In the AP600 DCD, each insight receives a disposition such as a reference to another portion of the DCD, an ITAAC, or a combined license (COL) information item. Table 19.1-102, "Summary of Insights from the PRA of the U.S. EPR," does not include a similar disposition for each insight to ensure that the assumptions remain valid in the as-to-be-built, as-to-be-operated plant. For example, the diversity of the station blackout diesel generators is an important assumption that must be retained by future COL holders. Please update Table 19.1-102 to include a disposition for each insight and ensure that the table reflects all important assumptions and insights that must remain valid for future plants.

Response to Question 19-02:

A response to this question will be provided by May 30, 2008.

Question 19-03:

Section 19.1.4.1.1.4, "Data Analysis," lists unavailabilities of equipment due to testing and maintenance as a type of data required for the probabilistic risk assessment (PRA), but does not provide the source of test and maintenance unavailability estimates. Please discuss how test and maintenance unavailabilities were derived. Please discuss how plans for online maintenance (given the four-train redundancy of most systems) were addressed if generic data was used.

Response to Question 19-03:

In the DC phase of the PRA development (before test & maintenance procedures are developed and before plant experience is available), simple assumptions are made on test and maintenance unavailabilities. These assumptions, based on engineering judgment, are summarized below:

- Preventive Maintenance (PM) of 7 days per year is assumed for each train.
- Corrective Maintenance (CM) of 3 days is assumed for all operating trains.
- Corrective Maintenance (CM) of 9 days is assumed for all stand-by trains.

Generic data was not used because data would not be applicable to an advanced plant with a four-train redundancy of most systems.

Both preventive and corrective maintenance are modeled in the same basic event for each train, labeled as PM. All PM activities are defined on the train level, not on the divisional level, so PM on medium head safety injection (MHSI) Div 1 train and low head safety injection (LHSI) Div1 train are treated as separate PM activities. This is a conservative assumption because multiple trains in the same division could be taken out in the same time. It is assumed that maintenance will not be performed simultaneously on the trains from the different divisions. This is an acceptable non-conservative assumption because a corrective maintenance that occurs simultaneously between different divisions is expected to be infrequent with limited duration.

PM sensitivity cases are presented in multiple tables throughout Chapter 19.1 (for internal, flood, and fire events, as well as for all events) where it was assumed that one train/division of safety systems was taken out for all year by setting PM value to 1 for Train 3 (Sensitivity cases 8a). The increases in core damage frequency (CDF) reported in the tables are in some cases more than a factor of 2. These evaluations are performed assuming that PM activities on the other three trains are allowed to occur at the same time. If this conservative assumption is changed to a more realistic one: if one division is out for PM, no other divisions will be taken out, the increase in the CDF is significantly smaller (less than 20%).

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-04:

Please provide the generic failure probabilities and distribution parameters used for components in the PRA, with references to the data source, so that the NRC staff can confirm the statement in section 19.1.4.1.1.4, “Data Analysis,” that the data is “comparable to other U.S. data sources.”

Response to Question 19-04:

A comparison between the data used in the U.S. EPR PRA and other U.S. data sources (when these sources are available) is provided in Table 19-04-1. Sources of U.S. EPR data and sources used for comparison are defined in the FSAR subsection: Sources of Component Failure Data (page 19.1-40).

FSAR Impact:

The FSAR will not be changed as a result of this question.

Table 19-04-1—Data Comparison

Comp Type	System	Data Source	Failure Mode Description	Mean Failure on Demand	Mean Failure Rate	Dist. Type	Error Factor/ Alpha
Battery	Elec.	**EPR: ZEDB-6.2.4.01**	Battery 220V (25-2800Ah) - failure on demand	6.57E-04		Lognormal	8.4
		ALWR EPRI Data	Battery - failure to provide output on demand	5.00E-04			
Bus - Outdoor	Elec.	**EPR: EG&G-T4_JBOFL**	Outdoor bus - failure (general)		1.00E-06	Lognormal	10
		ALWR EPRI Data	Electrical buswork - failure during operation		2.00E-07		
Circuit Breaker - General	Elec.	**EPR: EG&G-T4_JABFC**	Circuit breaker - failure to close	5.00E-04		Lognormal	10
		ALWR EPRI Data	Circuit breaker (4kv) - failure to close	3.00E-04			
			Circuit breaker (≤600 v) - failure to close	1.00E-03			
Circuit Breaker - General	Elec.	**EPR: EG&G-T4_JABFO**	Circuit breaker - failure to open	5.00E-04		Lognormal	10
Circuit Breaker - General	Elec.	**EPR: EG&G-T4_JAOSO**	Circuit breaker - spurious operation		3.00E-07	Lognormal	10
Chiller Unit	QK, QNA	**EPR: EG&G-T3_CHFR**	Chiller - failure to run		3.00E-05	Lognormal	10
		ALWR EPRI Data	Room chiller unit - failure to run		1.00E-05		
Chiller Unit	QK	**EPR: EG&G-T3_CHFS**	Chiller - failure to start	5.00E-03		Lognormal	5
		ALWR EPRI Data	Room chiller unit - failure to start	6.00E-03			
Diesel Generator	XKA	**EPR: ZEDB-6.2.1.02 FR**	Diesel Generator (2682-5000KW) - failure to run		2.40E-03	Lognormal	7.3
		ALWR EPRI Data	Diesel Generator - failure to run		2.40E-03		
Diesel Generator	XKA	**EPR: ZEDB-6.2.1.02 FS**	Diesel Generator (2682-5000KW) - failure to start	4.50E-03		Lognormal	3.9
		ALWR EPRI Data	Diesel Generator - failure to start and load	1.40E-02			
Filter	PE	**EPR: EG&G-T1_FILPG**	Filter - plugs		5.00E-06	Lognormal	10
Fan	SAC	**EPR: ZEDB02-6.3.3.01 FR**	ZEDB (2002) Fan (0,1-0,4kW) - failure to run		2.11E-06	Lognormal	3.64
		ALWR EPRI Data	Blower/ventilation fan - failure to run		1.00E-05		
Fan	SAC	**EPR: ZEDB02-6.3.3.02 FR**	Fan (5.5-45kW) - failure to run		1.50E-05	Lognormal	12.4
		ALWR EPRI Data	Blower/ventilation fan - failure to run		1.00E-05		
Fan	PE	**EPR: EG&G-T3_VFR**	Ventilation fan - failure to run		3.00E-05	Lognormal	10
		ALWR EPRI Data	Blower/ventilation fan - failure to run		1.00E-05		
Fan	SAC	**EPR: ZEDB02-6.3.3.01 FS**	ZEDB (2002) Fan (0,1-0,4kW) - failure to start	8.93E-05		Lognormal	8.44
		ALWR EPRI Data	Blower/ventilation fan - failure to start	6.00E-04			
Fan	SAC	**EPR: ZEDB02-6.3.3.02 FS**	ZEDB (2002) Fan (5.5-45kW) - failure to start	2.19E-04		Lognormal	3.81
		ALWR EPRI Data	Blower/ventilation fan - failure to start	6.00E-04			
Fan	PE	**EPR: EG&G-T3_VFS**	Ventilation fan - failure to start	5.00E-03		Lognormal	5
		ALWR EPRI Data	Blower/ventilation fan - failure to start	6.00E-04			
Heat Exchanger - Shell	KA, PG, XJ	**EPR: EG&G-T1_EXSEL**	Heat exchanger shell - external leakage		3.00E-07	Lognormal	10
		ALWR EPRI Data	Heat exchanger - failure while operating (leaks, plugs)		1.00E-06		
Heat Exchanger - Tube	LAD, LCS	**EPR: EG&G-T1_EXTEL**	Heat exchanger - tube leakage		1.00E-06	Lognormal	10
		ALWR EPRI Data	Heat exchanger - failure while operating (leaks, plugs)		1.00E-06		
Heat Exchanger	JMQ,	**EPR: EG&G-T1_EXTLK**	Heat exchanger - tube leakage		1.00E-06	Lognormal	10

Table 19-04-1—Data Comparison

Comp Type	System	Data Source	Failure Mode Description	Mean Failure on Demand	Mean Failure Rate	Dist. Type	Error Factor/ Alpha
- Tube	JNG, KA	ALWR EPRI Data	Heat exchanger - failure while operating (leaks, plugs)		1.00E-06		
Input Module	I&C	**EPR: S466 SM**	Analog input module (self monitored) - failure		1.10E-06	Lognormal	5
Output Module	I&C	**EPR: S470 BP**	Analog output module (self monitored) - failure		1.51E-08	Lognormal	5
Signal Modifier	I&C	**EPR: SAA1 NS**	Analog signal modifier (non-self monitored) - failure		1.07E-07	Lognormal	5
Signal Modifier	I&C	**EPR: SAA1 SM**	Analog signal modifier (self monitored) - failure		1.07E-07	Lognormal	5
Backplane	I&C	**EPR: SBG5 SM**	Backplane subrack (self monitored) - failure		9.25E-06	Lognormal	5
Backplane	I&C	**EPR: SBG6 SM**	Backplane subrack (half of split rack) (self monitored) - failure		9.08E-06	Lognormal	5
Communication Module	I&C	**EPR: SL21 BP**	Communication module - failure		3.32E-08	Lognormal	5
Communication Module	I&C	**EPR: SL21 SM**	Communication module (self monitored) - failure		8.52E-07	Lognormal	5
Counter Module	I&C	**EPR: S706 SM**	Counter module (self monitored) - failure		1.30E-06	Lognormal	5
Input Module	I&C	**EPR: S430 NS**	Digital input module (non-self monitored) - failure		7.92E-08	Lognormal	5
Input Module	I&C	**EPR: S430 SM**	Digital input module (self monitored) - failure		1.56E-08	Lognormal	5
Output Module	I&C	**EPR: S451 NS**	Digital output module (non-self monitored) - failure		3.91E-07	Lognormal	5
Output Module	I&C	**EPR: S451 SM**	Digital output module (self monitored) - failure		3.60E-07	Lognormal	5
Priority Module	I&C	**EPR: AV42 NS**	Priority module (non-self monitored) - failure		3.25E-07	Lognormal	5
Priority Module	I&C	**EPR: AV42 SM**	Priority module (self monitored) - failure		3.25E-07	Lognormal	5
Processor Module	I&C	**EPR: SVE2 NS**	Processor module (non-self monitored) - failure		7.61E-09	Lognormal	5
Processor Module	I&C	**EPR: SVE2 SM**	Processor module (self monitored) - failure		7.53E-07	Lognormal	5
Power Rack	I&C	**EPR: PWR RACK SM**	Accupulse 24V DC power supply rack - failure		5.00E-06	Lognormal	5
Relay	I&C	**EPR: SRB1 FD**	Relay - failure to de-energize	2.32E-06		Lognormal	5
Relay	I&C	**EPR: SRB1 FE**	Relay - failure to energize	1.16E-04		Lognormal	5
Sensor - Level	I&C	**EPR: SENSOR-LEVEL**	Level sensor and transmitter - failure		2.15E-06	Lognormal	5
		ALWR EPRI Data	Flow transmitter - failure to respond to change in process flow		4.60E-07		
			Pressure transmitter - failure to respond to change in process pressure		4.80E-07		
			Level transmitter - failure to respond to change in level		1.00E-06		
			Temperature transmitter - failure to respond to change in process temperature		3.50E-07		
Sensor - Pressure	I&C	**EPR: SENSOR-PRESSURE**	Pressor sensor and transmitter - failure		1.08E-06	Lognormal	5
		ALWR EPRI Data	Flow transmitter - failure to respond to change in process flow		4.60E-07		
			Pressure transmitter - failure to respond to change in process pressure		4.80E-07		

Table 19-04-1—Data Comparison

Comp Type	System	Data Source	Failure Mode Description	Mean Failure on Demand	Mean Failure Rate	Dist. Type	Error Factor/ Alpha
			Level transmitter - failure to respond to change in level		1.00E-06		
			Temperature transmitter - failure to respond to change in process temperature		3.50E-07		
Sensor - Temperature	I&C	**EPR: SENSOR-TEMPERATURE**	Temperature sensor and transmitter - failure		6.95E-06	Lognormal	5
		ALWR EPRI Data	Flow transmitter - failure to respond to change in process flow		4.60E-07		
			Pressure transmitter - failure to respond to change in process pressure		4.80E-07		
			Level transmitter - failure to respond to change in level		1.00E-06		
			Temperature transmitter - failure to respond to change in process temperature		3.50E-07		
Signal Modifier	I&C	**EPR: SCV1 NS**	Signal conditioner module (non-self monitored) - failure		2.61E-07	Lognormal	5
Signal Modifier	I&C	**EPR: SCV1 SM**	Signal conditioner module (self monitored) - failure		2.61E-07	Lognormal	5
Signal Multiplier	I&C	**EPR: SNV1 NS**	Signal multiplier (non-self monitored) - failure		2.03E-07	Lognormal	5
Signal Multiplier	I&C	**EPR: SNV1 SM**	Signal multiplier (self monitored) - failure		2.03E-07	Lognormal	5
Inverter	Elec.	**EPR: ZEDB_6.2.6-3_FR**	Inverter 400V (86,5-207,6 kVA) - failure to run		1.25E-06	Lognormal	5.19
		ALWR EPRI Data	Inverter - failure during operation		2.00E-05		
Pump - Motor Driven	KA, LAS, PG, QK, QNA	**EPR: EG&G-T1_POEEL**	Motor-driven pump - external leakage		3.00E-06	Lognormal	10
Pump - Motor Driven	KA	**EPR: ZEDB-6.2.2.06 FR**	Pump (25-120m; 590-1389kg/s) - failure to run		2.00E-06	Lognormal	8.44
		ALWR EPRI Data	Motor-driven pump (comp. cooling) - failure to run		5.00E-06		
			Motor-driven pump (all types) - failure to run		2.50E-05		
Pump - Motor Driven	KBA	**EPR: ZEDB-6.2.2.01 FR**	Pump (1680-1730mm;5.6-10kg/s) - failure to run		1.30E-05	Lognormal	3.63
		ALWR EPRI Data	Motor-driven pump (all types) - failure to run		2.50E-05		
Pump - Motor Driven	GHC, KA	**EPR: EG&G-T1_POEFR**	Motor-driven pump - failure to run		3.00E-05	Lognormal	10
		ALWR EPRI Data	Motor-driven pump (all types) - failure to run		2.50E-05		
Pump - Motor Driven	JND, LA, LAJ, LAS	**EPR: ZEDB-6.2.2.03A FR**	Pump (285-1070m;16.7-80kg/s) - failure to run		5.10E-04	Lognormal	7.08
		ALWR EPRI Data	Motor-driven pump (emergency feed) - failure to run		1.50E-04		
			Motor-driven pump (all types) - failure to run		2.50E-05		
Pump - Motor Driven	JMQ, JNG, KA, PE, QK, QNA	**EPR: ZEDB-6.2.2.04 FR**	Pump (15-165m; 0.6-195kg/s) - failure to run		1.01E-05	Lognormal	3.24
		ALWR EPRI Data	Motor-driven pump (LPI/RHR) - failure to run		1.00E-05		
			Motor-driven pump (safety inj.) - failure to run		5.00E-05		
			Motor-driven pump (cont. spray) - failure to run		5.00E-05		
			Motor-driven pump (comp. cooling) - failure to run		5.00E-06		
			Motor-driven pump (service water) - failure to run		3.20E-05		
			Motor-driven pump (all types) - failure to run		2.50E-05		

Table 19-04-1—Data Comparison

Comp Type	System	Data Source	Failure Mode Description	Mean Failure on Demand	Mean Failure Rate	Dist. Type	Error Factor/ Alpha
Pump - Motor Driven	PC, PE, PG	**EPR: ZEDB-6.2.2.11 FR**	Pump (10-71m; 694-1530kg/s) - failure to run		4.60E-06	Lognormal	3.79
		ALWR EPRI Data	Motor-driven pump (comp. cooling) - failure to run		5.00E-06		
			Motor-driven pump (service water) - failure to run		3.20E-05		
			Motor-driven pump (all types) - failure to run		2.50E-05		
Pump - Motor Driven	JDH	**EPR: ZEDB-6.2.2.17 FR**	Piston pump (887-2500mm; 1.4-6.25kg/s) - failure to run		6.14E-04	Lognormal	7.16
		ALWR EPRI Data	Motor-driven pump (all types) - failure to run		2.50E-05		
Pump - Motor Driven	KA	**EPR: ZEDB-6.2.2.06 FS**	Pump (25-120m; 590-1389kg/s) - failure to start	1.39E-03		Lognormal	3.8
		NUREG 1715 Data	Motor-driven pump - failure to start	1.35E-03			
		ALWR EPRI Data	Motor-driven pump (comp. cooling) - failure to start	1.30E-03			
			Motor-driven pump (all types) - failure to start	2.00E-03			
Pump - Motor Driven	KBA	**EPR: ZEDB-6.2.2.01 FS**	Pump (1680-1730mm; 5.6-10kg/s) - failure to start	9.81E-04		Lognormal	4.06
		NUREG 1715 Data	Motor-driven pump - failure to start	1.35E-03			
		ALWR EPRI Data	Motor-driven pump (all types) - failure to start	2.00E-03			
Pump - Motor Driven	GHC, KA	**EPR: EG&G-T1_POEFS**	Motor-driven pump - failure to start (breaker included)	3.50E-03		Lognormal	10
		NUREG 1715 Data	Motor-driven pump - failure to start	1.35E-03			
		ALWR EPRI Data	Motor-driven pump (all types) - failure to start	2.00E-03			
Pump - Motor Driven	JND, LA, LAJ, LAS	**EPR: ZEDB-6.2.2.03A FS**	Pump (285-1070m;16.7-80kg/s) - failure to start	1.28E-03		Lognormal	6.11
		NUREG 1715 Data	Motor-driven pump - failure to start	1.35E-03			
		ALWR EPRI Data	Motor-driven pump (safety inj.) - failure to start	1.00E-03			
			Motor-driven pump (emergency feed) - failure to start	3.00E-03			
			Motor-driven pump (all types) - fails to start	2.00E-03			
Pump - Motor Driven	JMQ, JNG, KA, PE, QK, QNA	**EPR: ZEDB-6.2.2.04 FS**	Pump (15-165m;0.6-195kg/s) - failure to start	4.02E-04		Lognormal	3.92
		NUREG 1715 Data	Motor-driven pump - failure to start	1.35E-03			
		ALWR EPRI Data	Motor-driven pump (LPI/RHR) - failure to start	2.30E-03			
			Motor-driven pump (safety inj.) - failure to start	1.00E-03			
			Motor-driven pump (cont. spray) - failure to start	5.00E-03			
			Motor-driven pump (comp. cooling) - failure to start	1.30E-03			
			Motor-driven pump (service water) - failure to start	2.40E-03			
			Motor-driven pump (all types) - failure to start	2.00E-03			
Pump - Motor Driven	PC, PE, PG	**EPR: ZEDB-6.2.2.11 FS**	Pump (10-71m;694-1530kg/s) - failure to start	1.33E-02		Lognormal	11.65
		NUREG 1715 Data	Motor-driven pump - failure to start	1.35E-03			
		ALWR EPRI Data	Motor-driven pump (comp. cooling) - failure to start	1.30E-03			
			Motor-driven pump (service water) - failure to start	2.40E-03			
			Motor-driven pump (all types) - failure to start	2.00E-03			
Pump - Motor Driven	JDH	**EPR: ZEDB-6.2.2.17 FS**	Piston pump (887-2500mm; 1.4-6.25kg/s) - failure to start	9.21E-04		Lognormal	4.48
		ALWR EPRI Data	Motor-driven pump (all types) - fails to start	2.00E-03			
Rectifier	Elec.	**EPR: ZEDB_6.2.6-1_FR**	Rectifier 220V (10-1000A) - failure to operate		6.39E-06	Lognormal	5.02
		ALWR EPRI Data	Inverter - failure during operation		2.00E-05		

Table 19-04-1—Data Comparison

Comp Type	System	Data Source	Failure Mode Description	Mean Failure on Demand	Mean Failure Rate	Dist. Type	Error Factor/ Alpha
Stand still seal	JE	**EPR: JEB_SSSF**	Stand-still seal - mechanical failure	1.00E-03		Beta	0.5
Strainer	JNK	**EPR: SUMP STRAINER**	Sump strain - plugged		5.00E-07	Lognormal	10
Switch	Elec.	**EPR: EG&G-T4_SWSFC**	Switch - failure to close	1.00E-05		Lognormal	5
Switch	Elec.	**EPR: EG&G-T4_SWSFO**	Switch - failure to open	1.00E-05		Lognormal	5
Switch	Elec.	**EPR: EG&G-T4_SWSSO**	Switch - spurious operation	1.00E-06		Lognormal	10
Tank	GHC, JDH, KA, LA	**EPR: EG&G-T1_BATEL**	Tank - external leakage		5.00E-07	Lognormal	10
		ALWR EPRI Data	Tank - fails catastrophically		1.00E-07		
Tank	LAR	**EPR: EFW TANK LEAK**	EFW tank leakage	1.00E-06		Lognormal	10
		ALWR EPRI Data	Tank - fails catastrophically		1.00E-07		
Transformer	Elec.	**EPR: EG&G-T4_TREFL**	Transformer - failure in operation		1.00E-06	Lognormal	10
		ALWR EPRI Data	Transformer (high voltage) - failure to continue operating		1.20E-06		
			Transformer (main step-up) - failure to continue operating		5.40E-06		
			Transformer (4 kv to 600/480 v) - failure to continue operating		7.00E-07		
			Transformer (lower voltage) - failure to continue operating		8.00E-07		
Valve - Check	KBA, PC, PG, SAC	**EPR: EG&G-T1_VACFC**	Check valve - failure to close	1.00E-03		Lognormal	5
		ALWR EPRI Data	Check valve (other than stop) - failure to close	1.00E-03			
			Stop-check valve - failure to operate on demand	2.00E-03			
Valve - Check	GHC, JDH, JE, JMQ, JND, JNG, KA, KBA, LA, LAH, LAR, PC, PE, PG, QK, QNA, SAC	**EPR: EG&G-T1_VACFO**	Check valve - failure to open	5.00E-05		Lognormal	5
		ALWR EPRI Data	Check valve (other than stop) - failure to open	2.00E-04			
			Stop-check valve - failure to operate	2.00E-03			
Valve - Check	JNG	**EPR: ZEDB-6.2.3.32 FO**	Check valve (> DN50) - failure to open	9.63E-04		Lognormal	3.41
		ALWR EPRI Data	Check valve (other than stop) - failure to open	2.00E-04			
			Stop-check valve - failure to operate	2.00E-03			
Valve - Check	GHC, JDH, JE, JEW, JMQ, JND, JNG, KA,	**EPR: ALWR CV FTRO**	Check valve - failure to remain open		2.00E-07	Lognormal	10
		ALWR EPRI Data	Check valve - failure to remain open		2.00E-07		

Table 19-04-1—Data Comparison

Comp Type	System	Data Source	Failure Mode Description	Mean Failure on Demand	Mean Failure Rate	Dist. Type	Error Factor/ Alpha
	KBA, LA, LAH, LAR, PC, PE, PG, QK, QNA, SAC						
Valve - Check	JND, JNG, KA, LA, LAH, PC, PE, PG, SAC	**EPR: EG&G-T1_VACIR**	Check valve - internal rupture		5.00E-07	Lognormal	10
		ALWR EPRI Data	Check valve - internal rupture		5.00E-09		
Valve - Manual	GHC, JDH, JMQ, JND, KA, KBA, LAH, LAR, LB, PE, PG, QK, QNA	**EPR: VAMEC1**	Valve left in wrong position (pre-acc. hum. err. manual valve cat. 1)	2.00E-04		Lognormal	10
Valve - Manual	GHC, JND, JNG	**EPR: PRE-ACCIDENT CAT 3**	Valve left in wrong position (pre-accident human error - cat. 3 - no test to verify)	8.00E-03		Lognormal	10
Valve - Motor Operated	JNG, LA, LAR, LB	**EPR: ZEDB-6.2.3.01 CF**	MS-Relief valve - failure to control flow		4.47E-06	Lognormal	5.51
Valve - Motor Operated	JE, JMQ, JNG, KA, KBA, LA, LB, LCQ	**EPR: EG&G-T1_VAEFC**	Motor-operated valve - failure to close (breaker included)	3.50E-03		Lognormal	5
		NUREG 1715 Data	Motor-operated valve - failure to close	4.60E-04			
		ALWR EPRI Data	Motor-operated valve - Fails to operate on demand	4.00E-03			
Valve - Motor Operated	JDH, JE, JMQ, JNA, JNK, KA, KBA, PE, SAC	**EPR: EG&G-T1_VAEFO**	Motor-operated valve - failure to open (breaker included)	3.50E-03		Lognormal	10
		NUREG 1715 Data	Motor-operated valve - failure to open	7.62E-04			
		ALWR EPRI Data	Motor-operated valve - fails to operate	4.00E-03			
Valve - Motor Operated	JDH, JE, JNA, JND, JNG, KA, KBA, LA, LB, LCQ, PE, PG	**EPR: EG&G-T1_VAEIR**	Motor-operated valve - internal rupture		1.00E-07	Lognormal	10

Table 19-04-1—Data Comparison

Comp Type	System	Data Source	Failure Mode Description	Mean Failure on Demand	Mean Failure Rate	Dist. Type	Error Factor/ Alpha
Valve - Motor Operated	GHC, JDH, JE, JEW, JMQ, JNA, JND, JNG, JNK, KA, KBA, LA, LAH, LB, LCQ, PE, PG, QK, QNC,SAC	**EPR: EG&G-T1T4_VAESO**	Motor-operated valve + breaker - spurious operation		3.50E-07	Lognormal	10
Valve - Pneumatic	LA, LAH	**EPR: EG&G-T1_VAPCF**	Pneumatic valve - failure to control flow (failure to open/close)	1.00E-03		Lognormal	10
Valve - Pneumatic	LB	**EPR: ZEDB-6.2.3.03 FC**	MS-Relief isolation valve (DN350) - failure to close	9.98E-04		Lognormal	8.44
		ALWR EPRI Data	Safety/relief valve (BWR, actuation mode) - failure to reclose	6.50E-03			
Valve - Pneumatic	LB	**EPR: ZEDB-6.2.3.02 FC**	MS isolation valve - failure to close	1.20E-03		Lognormal	8.44
Valve - Pneumatic	KA, LA, LB	**EPR: EG&G-T1_VAPFC**	Pneumatic valve - failure to close (breaker included)	1.50E-03		Lognormal	10
		NUREG 1715 Data	Air-operated valve - failure to close	5.14E-04			
		ALWR EPRI Data	Air-operated valve - failure to operate	2.00E-03			
Valve - Pneumatic	KA, LA, LB	**EPR: EG&G-T1_VAPFO**	Pneumatic valve - failure to open (incl. breaker)	1.50E-03		Lognormal	10
		NUREG 1715 Data	Air-operated valve - failure to close	5.14E-04			
		ALWR EPRI Data	Air-operated valve - failure to operate	2.00E-03			
Valve - Pneumatic	LB	**EPR: ZEDB-6.2.3.03 FO**	MS-Relief isolation valve (DN350) - failure to open	3.55E-03		Lognormal	2.95
		ALWR EPRI Data	Safety/relief valve (BWR, actuation mode) - failure to open	6.00E-03			
Valve - Pneumatic	JE, KA, LA, LB	**EPR: EG&G-T1T4_VAPSO**	Pneumatic valve + breaker - spurious operation		3.30E-06	Lognormal	10
		ALWR EPRI Data	Air-operated valve - transfers closed		1.50E-07		
Valve - Relief	JNG, LA, LAR, LB	**EPR: ZEDB-6.2.3.01 CF**	MS-Relief valve - failure to control flow	1.50E-03		Lognormal	5.51
Valve - Relief	JE	**EPR: EIREDA95_T70_SFO**	Pilot-operated safety relief valve - failure to open	2.10E-04		Beta	2.86
Valve - Safety	LB	**EPR: EIREDA95_T74_SFO**	MS safety valve (spring load) - failure to open	4.69E-04		Beta	20
Valve - Safety	JDH, JE, JNA, JNG, KA, KBA, LB, PG	**EPR: EG&G-T1_VASPO**	Safety valve - premature opening		3.00E-06	Lognormal	10
Valve - Safety	LB	**EPR: EG&G-T1_VASRC**	Safety valve - failure to reclose	3.00E-03		Lognormal	5

Table 19-04-1—Data Comparison

Comp Type	System	Data Source	Failure Mode Description	Mean Failure on Demand	Mean Failure Rate	Dist. Type	Error Factor/ Alpha
Valve - Solenoid	JE	**EPR: EIREDA95_T70_VAFC**	Solenoid valve - failure to close	2.10E-04		Beta	2.86
Valve - Solenoid	JE, KA, LB	**EPR: EG&G-T1_VAOFC**	Solenoid valve - failure to close	5.00E-04		Lognormal	10
Valve - Solenoid	JE, KA, LA, LB	**EPR: EG&G-T1_VAOFO**	Solenoid valve - failure to open	5.00E-04		Lognormal	10
Valve - Solenoid	JE, KA, LA, LB	**EPR: EG&G-T1_VAOSO**	Solenoid valve - spurious operation		5.00E-07	Lognormal	10

Question 19-05:

The values presented in the "Risk Metrics" sections throughout Chapter 19 appear to be point estimates. NRC guidance, as well as the American Society of Mechanical Engineers (ASME) PRA standard, specifically requests mean values rather than point estimates. (See Regulatory Guide (RG) 1.174, section 2.2.5.5; RG 1.206, Section C.I.19, Appendix A; SRP 19.0, section III; ASME RA-Sb-2005, Supporting Requirement QU-A2b; and RG 1.200, Table A-1, clarification of requirement QU-A2b.)

Also, the uncertainty cases for which diesel generator uncertainty was eliminated are not appropriate. The footnote to the supporting requirement on uncertainty in the ASME PRA standard refers to a 1981 paper (G. Apostolakis and S. Kaplan, "Pitfalls in Risk Calculations," Reliability Engineering, Vol. 2, pp 135-145, 1981.) that identifies the importance of handling state-of-knowledge dependencies correctly because of the potential understatement of both the mean and variance of a probability distribution. The worst-case underestimation is a system with four redundant components, where the mean is underestimated by a factor of 300 and the 95th percentile by a factor of 25 for the simple example presented in the paper. The high mean for a probability distribution that includes redundant equipment failures is therefore an important insight, not an artifact that should be handled by removing uncertainty distributions on certain components.

Therefore, the final safety analysis report (FSAR) should be revised to reflect:
(a) Mean values for risk metrics (i.e., core damage frequency (CDF) and large release frequency (LRF)) in all appropriate sections,
(b) Any changes to risk insights or importance measures as a result of using the mean value,
(c) Clarified discussion of the impact of redundant equipment with the same state-of-knowledge-based probability distribution,
(d) Discussion of why the impact is different for the internal events, fire, flooding, shutdown and Level 2 PRA elements.

Additionally, the response to this question should include a list of the correlation classes used in the PRA model and the components that are assigned to each class. If there is any difference between the correlation class grouping and common cause grouping (especially for the emergency and station blackout diesel generators), please identify and justify these differences.

Response to Question 19-05:

The response to this question will be provided by May 30, 2008.

Question 19-06:

Section 19.1.4.1.1.4 states that point estimates (not mean values) were used for frequency inputs to the CDF quantification for initiating events whose frequencies were calculated using fault trees. Please provide the mean frequencies for all initiating events evaluated using fault trees. Please discuss how the state-of-knowledge correlation described above is addressed for these frequencies.

Response to Question 19-06:

The mean frequencies for all initiating events (IE) whose frequencies were calculated using fault trees are provided in Table 19-06-1. The state-of-knowledge relationship is accounted for by the multiple Monte Carlo simulations used to calculate these mean values. The total number of the simulations used to quantify the mean value was >350,000, which was accomplished by the multiple RS software runs (e.g., 32,000 simulations each) until the mean value stabilized.

As stated in Section 19.1.4.1.1.4, for these initiating events, point estimates, and not mean values, were used as inputs to the CDF point estimate quantification. However, the mean values were used as inputs to the CDF mean value quantification in the uncertainty runs. As demonstrated by the uncertainty curves in the FSAR, the change in the total CDF point estimate value, if the IE frequencies mean values are used instead of the point estimates, is negligible (<1E-8). In other words, the CDF point estimates on the uncertainty curves are the same as the CDF point estimates from the non-Monte Carlo RS output. This is because ISLOCAs are not significant contributors to the total risk, as shown in Table 19-06-1. This is also stated in the FSAR sensitivity analysis, Section 19.1.4.1.26, page 19.1-58.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Table 19-06-1—IE Mean Values and Uncertainty Parameters for IEs Modeled by Fault Trees

ID	Description	Point Estimate	Average (Based on 352,000 Monte Carlo simulations)				% Contribution to the Internal Events CDF
			Mean	95th	5th	Median	
IE 31BDA	Initiator - Loss of Divisional Emergency AC (Switchgear 31BDA)	3.49E-02	3.39E-02	1.28E-01	1.32E-03	1.31E-02	1.51%
IE ISL-CCW RCPTB	Initiator - ISLOCA - CCWS RCP Thermal Barrier Tube Break	4.13E-10	4.22E-10	1.19E-09	7.24E-15	8.65E-12	0.00%
IE ISL-CVCS HPTR	Initiator - ISLOCA - Tube Rupture High Pressure Letdown Cooler	9.17E-10	1.52E-08	8.86E-09	1.35E-13	4.80E-11	0.04%
IE ISL-CVCS INJ	Initiator - ISLOCA - High Pressure CVCS Pipe Rupture Outside Containment	6.25E-12	8.18E-11	1.64E-10	1.55E-14	1.60E-12	0.00%
IE ISL-CVCS REDS	Initiator - ISLOCA - Spurious Opening of Reducing Station	3.70E-10	1.80E-09	1.68E-09	3.98E-13	5.49E-11	0.02%
IE ISL-SIS LHSI	Initiator - ISLOCA - Break in LHSI Cold Leg Inj. CV with LHSI Line Break in Respective SAB	3.45E-11	2.35E-10	4.00E-10	2.43E-14	3.10E-12	0.01%
IE ISL-SIS MHSI	Initiator - ISLOCA - Break in MHSI Cold Leg Injection CV with MHSI Line Break in Respective SAB	3.45E-11	2.35E-10	4.00E-10	2.43E-14	3.10E-12	0.01%
IE ISL-SIS RHR	Initiator - ISLOCA - Fl of Suction Line Iso MOVs and Subsequent RHR Line Break in Respective SAB	7.87E-12	4.87E-11	6.23E-11	2.45E-15	3.54E-13	0.00%
IE LBOP	Initiator - Loss of Balance of Plant - Closed Loop Cooling Water or Aux Cooling Water	5.08E-02	4.89E-02	1.30E-01	1.05E-02	3.50E-02	1.92%
IE LOCCW-ALL	Initiator - Loss of CCWS/ESWS - Total Loss of 4 Divisions	2.46E-06	2.70E-06	9.74E-06	7.66E-08	8.60E-07	1.19%
IE LOCCW-CH1L	Initiator - Loss of CCWS/ESWS - Leak in Common Header 1	2.00E-01	1.68E-01	6.57E-01	7.88E-03	7.74E-02	2.67%
IE LOCCW1	Initiator - Loss of CCWS/ESWS Train 1 and Failure of Switchover	2.74E-03	2.84E-03	8.86E-03	3.99E-04	1.57E-03	0.08%

Table 19-06-1—IE Mean Values and Uncertainty Parameters for IEs Modeled by Fault Trees

ID	Description	Point Estimate	Average (Based on 352,000 Monte Carlo simulations)				% Contribution to the Internal Events CDF
			Mean	95th	5th	Median	
IE LOCCW12	Initiator - Loss of CCWS/ESWS Train 1 and Train 2	4.50E-03	4.40E-03	1.26E-02	8.84E-04	2.97E-03	0.86%
IE LOCCW12 PM2	Initiator - Loss of CCWS/ESWS Train 1 and Train 2, CCWS/ESWS2 in PM	1.80E-02	1.76E-02	5.04E-02	3.54E-03	1.19E-02	0.50%
IE LOCCW14-CH1	Initiator - Loss of CCWS/ESWS Trains 1 and 4 and Failure of Switchover to CH 1	1.72E-05	1.79E-05	6.42E-05	8.37E-07	7.53E-06	0.07%
IE LOCCW14-CH12	Initiator - Loss of CCWS/ESWS Trains 1 and 4 and Failure of Switchover to CH 1 & 2	2.23E-07	3.55E-07	1.05E-06	4.41E-09	5.91E-08	0.01%
IE LOCCW1L	Initiator - Leak in CCWS Train 1 and Failure to Isolate	5.32E-04	5.12E-04	1.91E-03	1.72E-05	1.49E-04	0.02%

Question 19-07:

Please provide system information (including a description and system drawing or fault tree) as assumed in the PRA for the closed cooling water system, auxiliary cooling water system, and operational chilled water system. These systems appear to be modeled in the PRA, but no information on the systems could be found in the rest of the FSAR.

Response to Question 19-07:

A response to this question will be provided by May 30, 2008.

Question 19-08:

Section 19.1.4.1.1.3, “Systems Analysis,” states that the Babcock & Wilcox (B&W) design most closely resembles the U.S. EPR in terms of total number of control rods and success criteria. Appendix C of NUREG/CR-5500, Volume 11, indicates that the control rod drive and rod failure data is based on pooled testing and unplanned trip data from B&W, Combustion Engineering (CE), and Westinghouse. Please discuss whether this pooling affects the conclusion that the B&W data is applicable to the U.S. EPR.

Response to Question 19-08:

NUREG/CR-5500, Volume 11 and the companion volumes for CE and Westinghouse PWRs all used the same failure experience to calculate the stuck control rod failure and CCF probabilities. The reason that the data is pooled is that the failure experience for control rod insertion failure is limited. The NUREG bases the control rod failure rate on one single control rod failure that occurred in the cumulative PWR experience (and a second added to cover uncertainty). The pooled denominator data covers a narrow span of time (nine years of unplanned trips, and six years of tests) relative to the overall industry experience. Consequently, the failure rate that is calculated for a single control rod failure is conservative and is essentially the same for all of the vendors.

Data pooling does not affect the conclusion of B&W data applicability to the U.S. EPR. The same pooled failure data that is used to calculate the random failure probability discussed above is also used to estimate the CCF probability. The variation in the CCF probabilities between vendor designs is primarily a function of the number of control rods in the plant, and the number of control rod insertions assumed for success (see response to Question 19-9). The data pooling is not a factor in the CCF variation that the NUREG reports between vendor designs.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-09:

Please provide more justification for the statement in section 19.1.4.1.1.3 that the control rod failure probability of 4.1E-8/demand from NUREG/CR-5500, Volume 11, is conservative for the U.S. EPR. The FSAR states that the U.S. EPR has 89 control rods, and analysis has shown that at least 38 control rods must fail to insert during a reactor trip before there is insufficient shutdown margin. This fraction—38 of 89 rods—corresponds to approximately 43%. It is not immediately obvious whether the common cause failure probability of 50% of 41 rods is greater than the failure probability of 38 of 89 rods. For comparison, Table E-7 of NUREG/CR-5500, Volume 11, provides a mean failure probability of 8.4E-7 for failure of 20% of rods (8/41) to insert.

Response to Question 19-09:

The CCF calculation in the NUREG is based on pooled industry failure data that includes only one control rod failure event (which involved a single control rod) and some other events involving control rod degradation. From this limited failure experience, a CCF probability is calculated and mathematically mapped to various control rod populations and CCF definitions involving from 7 to 20 control rods. This is a conservative data treatment considering the extension of the data to CCF events that have never occurred. As acknowledged in the NUREG, the mapping methodology works well when system sizes are close to one another, and overestimates the CCF probability when mapping up to a much larger population size.

NUREG/CR-5500, Volume 11 and the companion volumes for CE and Westinghouse contain several cases for the CCF definition, as shown in Table 19-09-1. In addition, the NUREG volumes contain sensitivity cases for CCF definitions ranging from three control rods (7.7e-6/demand) to 33 control rods (6.0 e-9/demand). The sensitivity studies show that the CCF probability decreases dramatically as the number of components increases.AREVA chose the case from the NUREG that was closest to the U.S. EPR success criteria. We view the failure probability for 20 control rods to be conservative relative to 38 failures. Given the extensive (and successful) control rod operating experience, the scarcity of failures, the conservative treatment in the NUREG, and the large number of control rod failures required for the U.S. EPR (38 of 89), this is considered to be a conservative approximation.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Table 19-09-1 Control Rod Insertion Failure CCFs in NUREG/CR-5500

Vendor	Number of control rods	Number of failed control rods	Calculated Probability (per demand)
Westinghouse	50	10	1.2e-6
Combustion Engineering	36	7	8.4e-7
		18	3.6e-8
Babcock & Wilcox	61 (41 credited in NUREG)	8	8.4e-7
		20	**4.1e-8**

Question 19-10:

Please provide justification for changing the level of dependence between post-maintenance testing and independent verification from complete to medium (section 19.1.4.1.1.5).

Response to Question 19-10:

The level of dependence between post-maintenance testing and independent verification was changed from complete to medium based on the assumptions that these two actions are likely to be performed in different time steps, with different crews; representing two different tasks. Based on the Fussell-Vesely importance value for this specific PRA input (a valve left in wrong position post T&M), an impact of this modification on the CDF is estimated as not significant (less than 5% impact on the total CDF).

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-11:

Please provide a more detailed description of Plant Operating State (POS) D, which section 19.1.6.1.2 describes as "RHR [residual heat removal] heat removal at mid-loop with RPV [reactor pressure vessel] head off." Commonly, water level is increased to the height of the RPV head flange before lifting the head, and the filling and draining POS are assessed separately from the mid-loop POS. Please describe any plans to operate at mid-loop with the RPV head off.

Response to Question 19-11:

The decision to operate at mid-loop with the RPV head off will be made by the COL applicant.

In the low power shutdown (LPSD) PRA model, the RCS level is assumed to be at mid-loop when RPV head is off in POS D. This assumption, which is conservative relative to time-to-boil, was selected to account for various ways outages could be conducted. The filling and draining of the cavity are also conservatively assigned to the same POS to simplify modeling.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-12:

Please explain how the U.S. EPR design has considered the Shutdown Management Guidelines in NUMARC 91-06, including how containment closure can be achieved in sufficient time to prevent potential fission product release (NUMARC Guidelines 4.5).

Response to Question 19-12:

NUMARC 91-06 guidelines have not yet been applied to a four-train RHR plant where loss of RHR is much less likely. However, the assumptions used in the PRA model with regard to assumed accident mitigating availability are reasonable for the design certification PRA. As described in Section 4.5 of NUMARC 91-06, procedures, training and alarms are called for in the guidance to ensure containment closure. This will be addressed in the pre-operational phase PRA and the PRA review process as described by FSAR COL item 19.1-9. Also, as described by this guidance, timing (decay heat level and water inventory) is an important consideration with regard to assuring containment closure before release.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-13:

Please provide a justification for not including support system failures, such as loss of component cooling water (CCW) or loss of essential service water (ESW), as initiating events in the shutdown PRA, as described in section 19.1.6.1.3. If support system failures are included as part of the loss of RHR initiating event, please discuss how the model accounts for the subsequent unavailability of these support systems after their failure causes a loss of RHR.

Response to Question 19-13:

Support system failures, such as loss of component cooling water (CCW) or loss of essential service water (ESW), are included as part of the loss of RHR initiating event in the SD PRA model. The SD PRA model accounts for the subsequent unavailability of these support systems after their failure causes a loss of RHR by merging IE fault trees with the mitigating system fault trees. This integration/merging was accomplished by selecting IEs mission time of 24 hours, the same as for the mitigating systems/functions, so that identical basic events are used in the IE and the system fault trees. A scaling to an actual IE mission time was accomplished by multiplying IE fault tree with the corresponding POS duration in days per year.

This concept of the IE fault trees with 24 hours mission time (multiplied by the POS duration in days/year) provides a solution for complex and multiple dependencies between “loss of RHR” initiating event and subsequent mitigating functions. The fault tree merging would also handle common cause concerns, if any are introduced.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-14:

Please provide further justification for not including low temperature overpressure events as initiating events in the shutdown PRA, as described in section 19.1.6.1.3. What would the impact be of the inadvertent start of a charging pump, given that charging pumps are not required to be isolated per LCO 3.4.11? The statement in section 19.1.6.1.7 that charging is not credited in shutdown does not imply that charging is not available. The probabilities of both the initiator and subsequent relief valve failures should be considered in the assessment.

Response to Question 19-14:

LTOP events are not included in the LPSD PRA because they have not been identified as SD initiating events that could significantly contribute to risk, as discussed in Section 19.1.6.1.3 for inadvertent start of RCP or MHSI pump. Similarly, over pressurization with charging when the pressurizer is solid is not judged to be a significant risk contributor. The reasons for that, and an evaluation, are summarized below:

- Spurious over pressure is judged unlikely.
- Exposure time with pressurizer solid is small (estimated less than 10 hours).
- Charging capacity is less than a MHSI or RCP pump, which means that operators may have an opportunity to trip the pumps before a significant over pressure occurs.
- There are three PSVs and one RHR suction relief valve at each RHR train to protect the system from overpressure.
- An overpressure event would likely result in a LOCA that still could be mitigated with secondary cooling and one MHSI pump. Thus, core damage would require failure of redundant mitigating systems.

Based on the above, this event is judged to be unlikely. The following provides a rough estimate for this type of scenario:

- IEF (initiating event frequency): assumed to be bounded by a human error, estimated to be on the order of 1E-2/year (assuming one PRZ solid configuration per year).
- ET (exposure time): 10 hours/year (not used because human error is estimated on demand).
- One of two PSVs (two reset for the LTOP regime) fails to open: 2E-5/demand (0.1*2E-4), one of three operating RHR train relief valves 6E-6/demand (0.3*0.1*2E-4).
- Estimated CDF (conservatively assuming that no mitigation will be available): IEF * PSVs* RHR RVs = 1.2E-12/yr.

This estimated LTOP CDF is smaller than 0.1% of the total SD CDF; therefore, inclusion in the analysis is not warranted.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-15:

Is the loss of offsite power (LOOP) frequency in the shutdown PRA assumed to be the same as the at-power LOOP frequency? Please describe any related assumptions, such as switchyard maintenance during shutdown.

Response to Question 19-15:

The LOOP frequency in the shutdown PRA is not the same as the at-power LOOP frequency. The SD LOOP frequency is 0.2/reactor shutdown year based on NUREG/CR-6890. This value is assumed to include a contribution from switchyard maintenance.

The values used in the U.S. EPR SD PRA and the corresponding sources are defined below:

- Shutdown LOOP Frequency (NUREG/CR-6890, Table 3-1): 1.96E-01/sdyr.
- SD LOOP non-recovery probability in 1hr (NUREG/CR-6890, Table 4-1, Composite): 0.413.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-16:

How does the shutdown PRA model account for both system-related failures (e.g., pump failures) and LOOP-related failures of the RHR system, and how are these failures separated to provide statements about the contribution of LOOP to shutdown risk?

Response to Question 19-16:

The shutdown PRA model accounts for both system-related failures (e.g., pump failures) and LOOP-related failures of the RHR system by merging IE and functional event fault trees.

As discussed in the response to Question 19-13, in order to integrate/merge IE fault trees with the mitigating system fault trees, the IE mission times were set to 24 hours. The IE “Loss of RHR” fault tree represents a full scope RHR fault tree including all hardware (pumps) and support failures (electric, cooling). An offsite power is a basic event in this fault tree (given for 24 hours, and than multiplied by the corresponding POS duration in days per year). The LOOP percentage contribution is estimated based on the FV value for this LOOP basic event. Note that this contribution includes total offsite power contribution through all systems that require electric power. The LOOP modeling in shutdown is also discussed in the response to Question 19-17.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-17:

How does the shutdown PRA model account for the subsequent unavailability of offsite power to support systems following a LOOP-induced loss of RHR?

Response to Question 19-17:

The shutdown PRA model accounts for the subsequent unavailability of offsite power to support systems following a LOOP-induced loss of RHR by merging IE and functional event fault trees.

As discussed in the responses to Question 19-13 and Question 19-16, in the shutdown model, the IE fault trees are merged with the mitigating system fault trees. That integration/merging was accomplished by selecting IEs mission time of 24 hours, the same as for the mitigating systems/functions, so that identical basic events are used in the IE and system fault trees. A scaling to an actual IE mission time was accomplished by multiplying IE fault tree with the corresponding POS duration in days per year. This modeling allows for inclusion of the support system failures (including a LOOP) as part of the loss of RHR initiating event. The model simply accounts for the subsequent unavailability of offsite power (in the corresponding functional events) by the fault tree merging.

Multiple examples of this application are illustrated in FSAR Table 19.1-92, U.S. EPR Important Cutset Groups – Level 1 Shutdown. Group 5 for example, describes a loss of RHR due to an unrecoverable LOOP. Note: LOOP events recovered in less than one hour are not considered in the analysis.

In the cutset shown in the table to represent Group 5:

- IE SD RHR CBD – presents only duration of the POS CBD: 2 (days/year),
- SD LOOP 24+REC – is the basic event from the RHR fault tree, for 24 hours (with recovery), which when multiplied by IE SD RHR CBD of 2 (days/year), represents total LOOP frequency for POS CBD, leading to a loss of RHR.

The rest of the basic events in this cutset define the other failures included in this group, and are described in FSAR Table 19.1-92.

This concept of the IE fault trees with 24 hours mission time (multiplied by the POS duration in days/year) provides a solution for complex and multiple dependencies between “loss of RHR” initiating event and subsequent mitigating functions.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-18:

Please justify the assumption in section 19.1.6.1.6 that all performance shaping factors (PSF) for operator actions are assumed to be optimal.

Response to Question 19-18:

The use of the word “optimal” in Section 19.1.6.1.6 refers to the use of nominal PSFs and does not convey any assumption regarding the reliability of these actions.

HEPs evaluated for operator actions performed during shutdown were based only on the estimate of time available to perform them (timing PSF). All other PSFs are assigned a nominal value of 1. This assumption is based on the fact that the “nominal” value of 1 is recommended for use in the SPAR-H method (NUREG/CR-6883) when insufficient information is available to determine otherwise.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-19:

Please clarify the assumed refueling cycle and duration of shutdown. Table 19.1-91 indicates 18 days shut down per year, and the technical specifications (TS) bases in Chapter 16 refer to a 24-month refueling cycle. How have forced outages and maintenance outages, with or without entry into mid-loop conditions, been considered?

Response to Question 19-19:

The assumptions on SD duration made in the SD PRA are summarized below:

1. An 18-month refueling cycle.
2. 94% plant availability.
3. Normal Refueling Outage duration is 14 days, with a refueling cycle of 18 months, this averages to 9 days/year.
4. Forced outage rate is 5 days/year, 3 of these days are assumed to be in Mode 4 & 2 days in Mode 5.
5. Margin to match 94% availability is assumed, that results in 7 days/year, proportionally distributed between different modes (POSs).

Note: In the PRA SD is defined as part of Mode 4 below 250°F and Modes 5 and 6.

No assumptions have been made with respect to long duration outages (e.g., Turbine Generator Overhaul, ISI, etc), which would be expected approximately every ten years.

The above assumptions result in a total of 21 days/year in PRA shutdown modes, three of which are assumed to be in Core Offload (POS F), an assumed duration of all the other POSs is defined in FSAR Table 19.1-91 and it sums to 18 days. The main factor in determining shutdown duration in this phase is assumed plant availability (see bullet 5 above); therefore the refueling cycle length (18 verses 24 months) is not expected to have a large affect on the yearly average SD duration.

The above assumptions made on SD duration are consistent with industry practice and observed nuclear industry trends to reduce refueling outage times. According to data collected and analyzed by INPO, the average capacity factor for US nuclear plants in the 2007 was 91.5% and the corresponding loss rate (forced outage rate) was 1.4%.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-20:

Section 19.1.6.1.8 states that transient combustibles and maintenance activities are judged not to be significant for the protected RHR trains providing decay heat removal during shutdown. What is the impact of transient combustibles and maintenance activities on the fire and flood frequency for RHR support systems (such as CCW or ESW)? Are these systems similarly protected during shutdown? How are fire and flood barriers controlled during shutdown? How are transient combustibles controlled during shutdown?

Response to Question 19-20:

The risk from floods and fires is not quantified specifically for shutdown, because it was assumed to be enveloped by the flood and fire risk at power operation (calculated for all year). The main differences in the flood and fire hazards between shutdown and power operation are, as summarized in the question, control of the fire and flood barriers and transient combustibles, and impacts of ongoing maintenance activities.

Control of the fire and flood barriers is not expected to have a large impact on the risk during the shutdown. The bases is provided below separately for flood and fire.

Flood: The flood areas defined in the Internal Flooding PRA encompass a whole building. Only structural walls are credited as flood barriers for this analysis, below Elevation 0'0", so that there are no doors and penetrations are minimal. The wall between SB 1 and the FB (SB 4 and the FB respectively) is not credited as a flood barrier because of the presence of a door between those two buildings at Elevation -31'. Therefore, the integrity of the flood barriers credited in the Internal Flooding PRA is not likely to be challenged during shutdown. (Note: The doors that separate the Annulus from SB 2 and SB 3 at Elevation 0'0" are modeled in the Internal Flooding PRA as closed with a certain probability of failing due to the water column. These doors may be open during certain phases of shutdown, which would be a favorable situation compared to an unmitigated flood in the Annulus).

Fire: Most of the fire areas modeled in the Fire PRA encompass a whole building/area. In the Safeguard Buildings fire barriers other than structural walls are credited. FSAR Table 19.1-62 shows the fire areas that were credited in the fire PRA. Most of the fire areas of SB 1 are located on different floors from each other. Direct fire propagation between them could only occur via floor/ceiling fire barriers, the integrity of which is not likely to be compromised during shutdown. In case of a breach of a fire barrier, indirect fire propagation could occur via the stairways/air shafts. However, stairways and air shafts are distinct fire areas with no significant amount of combustible material in them and constitute a buffer between the fire areas modeled. Propagation to another floor is judged unlikely. For the fire areas credited in the PRA that share the same floor, there is a limited number of points where separation between two areas could be jeopardized and for these areas (AC & DC switchgear rooms) the impact on the PRA mitigating systems is very similar.

In the shutdown PRA an assumption was made that a control of transient combustibles and limiting maintenance activities would apply to a RHR operating train and supporting systems.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-21:

Please provide additional detail on the modeling of low-probability human failures in the shutdown PRA. What assumptions (such as procedures, cues, and timing) have been made, and how will these conditions be ensured in the as-to-be-operated plant? At a minimum, discuss the failure of the operator to isolate the chemical and volume control system (CVCS) low pressure reducing station (OPE-ISOCSLPRS) and the failure of the operator to start maintenance heating, ventilation, and air conditioning (HVAC) trains after failure of normal safety air chiller (SAC) safety train (OPF-SAC-1H).

Response to Question 19-21:

The LPSD PRA model includes the shutdown specific operator errors discussed in Section 19.1.6.1.6 as well as some operator errors from the at-power model. The low-probability human errors referred to in this question belong to both of those two categories, as described below.

Shutdown-specific HEPs:

- Shutdown-specific operator errors are evaluated based on the time available, with other PSFs being nominal, as explained in the response to question 19-18. The HEP is generally determined by its timing PSFs. For actions where five hours or more are available, “expansive” time is available for both diagnosis and action. For actions where more than eight hours are available, an additional PSF of 0.5 is included in the diagnosis and action HEP. The justification for this PSF is that during an eight hour time period a shift change is likely to occur. The change of crew significantly increases the chances of diagnosing and correcting the problem. This assumption results in a total HEP of 5.5E-05. Out of over 50 shutdown-specific operator actions modeled, two of them (OPE-ISOCSLPRS and OPF-ISORHRFD-E) have an available time of more than eight hours. Table 19-21-1 shows the PSFs and the resulting HEPs for the action OPE-ISOCSLPRS.

At-power HEPs used in shutdown:

- Operator errors that were carried over from the at-power model are assumed to have the similar cues, timing and procedures in the SD POSs. This assumption is judged to be valid for support systems (e.g., HVAC) that will be operated in a similar manner at power and during shutdown. This applies to OPF-SAC-1H, an operator error to start the maintenance HVAC train upon failure of the safety-related HVAC train. The cues for this action are specific indications of the failure of the safety-related system. Indications of overheating in the switchgear rooms is used as a cue for the next recovery action OP-SAC-2H. Table 19-21-2 shows the PSFs and the resulting HEPs for the action OPF-SAC-1H.

COL item 19.1-9 listed in FSAR Table 1.8-2 is provided to confirm that assumptions used in the PRA remain valid for the as-to-be-operated plant.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Table 19-21-1—PSFs and HEPs determination for OPE-ISOCSLPRS

ID	Description		Basic HEP	Time available (min)	Time Required (min)	Timing PSF	Additional PSF	HEP mean value
OPE-ISOCSLPRS	Operator Fails to Isolate the CVCS Low Pressure Reducing Station	Diagnosis	0.01	500	30	0.01	0.5	5.00E-05
		Action	0.001	500	5	0.01	0.5	5.00E-06
		Total						5.50E-05

Table 19-21-2—PSFs and HEP determination for OPF-SAC-1H

ID	Description		Basic HEP	Time available (min)	Time Required (min)	Timing PSF	Stress PSF	Complexity* PSF	Other PSFs	HEP mean value
OPF-SAC-1H	Operator Fails to Start Maintenance HVAC Trains After Failure of Normal SAC Safety Train	Diagnosis	0.01	60	5	0.01	1	1	1	1.00E-04
		Action	0.001	60	5	0.1	1	1	1	1.00E-04
		Total								2.0E-04

Question 19-22:

Please describe the proposed sequence of events during shutdown between entry into MODE 5 and installation of nozzle dams in the steam generators and during startup between removal of nozzle dams and entry into MODE 4.

Response to Question 19-22:

The decision to use nozzle dams will be made by the COL applicant.

No use of nozzle dams is considered in the shutdown PRA.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-23:

Table 19.1-87 indicates significant differences between the sub-states of POS CA (CAd1, CAd2, and CAd3), especially the mode, availability of steam generators for heat removal, and TS requirements. Therefore, please justify the modeling of POS CA as a single state and describe how available mitigation strategies in each of the sub-states are addressed in the detailed system modeling.

Response to Question 19-23:

The differences between the modeled CAd2 state and the other two states identified are not judged to be significant, as summarized below:

- CAd2 conservatively envelopes CAd3 conditions.
- CAd2 does not completely envelope CAd1 in a conservative way; however the differences are not significant. For example, only two RHR pumps are running in CAd1, which means that loss of RHR is more likely than modeled in CAd2 with all four pumps running. However, all four steam generators are available in CAd1 with the startup feedwater pump running. This means that loss of heat removal (RHR and steam generators) in CAd1 will be less likely than what is modeled in CAd2 when two steam generators and startup feedwater pump are assumed unavailable.

The simplified modeling choice of CAd2 is appropriate.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-24:

Please clarify when the steam generators can be used for heat removal, by both MODE and POS. Discuss how the availability of the steam generators will be ensured, given that:

(a) The steam generator tubes (LCO 3.4.16), emergency feedwater (EFW) system (LCO 3.7.5), and EFW storage pools (LCO 3.7.6) are required by TS only in MODES 1-4

(b) Steam generator pressure and level sensors, main steam safety valves (MSSVs), and main steam relief trains (MSRTs) are required by TS only in MODES 1-3 (LCOs 3.3.1, 3.7.1, and 3.7.4)

(c) Table 19.1-87 indicates that the RCS is vented in POS CAd2, CAd3, CB, and CAu

Response to Question 19-24:

Table 19-24-1 summarizes by mode and by plant operating state (POS) when the SGs are available for heat removal in the PRA.

The availability of steam generators for heat removal is based on typical risk management practices, past experience in the US industry and the fact that typically not all steam generators are taken out of service at the same time early in the outage when decay heat levels are relatively high.

All SGs (RCS loops) are required operable in Mode 3 with the control rods energized and two loops are required operable in Mode 3 with the control rods de-energized. SG cooling is credited in Chapter 15 in Modes 1 , 2 and 3 But not in Mode 4. In Mode 4 and lower, SG cooling is not credited. It is used for normal cooldown. The EFW system is cited as a Criterion 4 (operating experience) in Mode 4.

The PRA assumptions involving availability of the steam generators are based on administrative controls. The availability of steam generators in Modes 4, 5 and 6, as controlled by operating procedures, is at the discretion of the COL applicant. COL item 19.1-9 listed in FSAR Table 1.8-2 is provided to confirm that PRA assumptions on SG availability remain valid.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Table 19-24-1—Mode and State vs. Steam Generator Availability

Mode	POS	Steam Generators Available
1-3	A, B	4
4	CA	2
5	CA, CB	2
6	D, E	0 (head is off)

Question 19-25:

Is reflux cooling via the steam generators at mid-loop credited in the shutdown PRA? If so, please provide a justification.

Response to Question 19-25:

Reflux cooling via a steam generator with feed capability is a success path that is credited for POS CBd in the shutdown PRA. Reflux cooling is an inherent capability that exists in the mid-loop reactor coolant system configuration. For the PRA model, this capability is based qualitatively on the ability of one steam generator to remove decay heat at a reduced level via reflux cooling. The reduced decay heat level is that encountered at approximately 6-hours post shutdown. An entry into POS CBd is expected to occur around 36 hours into shutdown.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-26:

Discuss how the re-pressurization (if any) required to use the steam generators for heat removal during shutdown challenges temporary pressure boundaries such as nozzle caps or thimble seals.

Response to Question 19-26:

The decision to use temporary pressure boundaries for SG maintenance or other purposes will be at the discretion of the COL applicant.

While unlikely, there is a potential for RCS pressurization when using SGs as backup for RHR, which could affect temporary pressure boundaries such as nozzle dams. Operating plants are required to analyze this potential and to have procedures in place to evacuate all personnel from the reactor building, if re-pressurization should occur. Because the U.S. EPR has the flexibility to use the SGs as backup for RHR the same approach will be used.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-27:

Sections 5.4.7.2.1 and 19.1.6.1.7 describe design features to address shutdown and mid-loop operations. However, most of these features appear to have limited or no coverage in TS, as presented in the attached table (Table RAI-19-1). Considering this table, please: (a) Confirm the apparent treatment in TS and justify the inclusion or exclusion of the referenced systems and signals according to the four criteria in 10 CFR 50.36. If the analysis determines that the system or signal should not be included in TS, discuss how the availability of these features designed to reduce shutdown risk will be ensured. (b) Discuss how each feature is credited in the shutdown PRA. (c) Provide a sensitivity study for the shutdown PRA that credits only the mitigating systems that are required to be operable according to TS. This request is related to SECY-97-168, in which the staff concluded that the current level of shutdown safety was achieved by voluntary measures that are not required by current regulations, and that these measures could be withdrawn by licensees without NRC approval.

Table RAI-19-1. Treatment of Shutdown Design Features in the U.S. EPR

Design Feature Identified in Section 5.4.7.2.1	Apparent Treatment in Technical Specifications
Inherent redundancy in the design of the four trains safety-related U.S. EPR safety injection system (SIS)/RHRS, with each train having separate RCS connections.	• LCO 3.4.6, 3.4.7, and 3.4.8 address operability of two or three trains of RHR in MODES 4 and 5 • MHSI, in-containment refueling water storage tank (IRWST), CCW, ESW, safeguard building controlled area ventilation system (SBVS), and safeguard building ventilation system electrical division (SBVSED) are only required to be operable in MODES 1-4 per LCO 3.5.3, 3.5.4, 3.7.7, 3.7.8, 3.7.12, and 3.7.13.
Automatic stop of the LHSI [low head safety injection] pumps in RHR mode in the event of a low loop level or low delta-Psat (difference between the RCS hot leg temperature and the RCS hot leg saturation temperature).	• No reference to either signal or to an RHR pump trip caused by either signal could be found in Table 3.3.1-1 of LCO 3.3.1.
Manual opening and closure of the RHR suction isolation valves (in addition of interlocks) prevent unwanted RHR connection or isolation on irregular RCS pressure.	• LCO 3.3.1 requires the inputs to the P14 permissive (wide range hot leg temperature and pressure) in MODE 3, which includes the pressure-temperature condition at which P14 is satisfied.
Safety injection via MHSI with reduced discharge head during low loop level ensures availability of the LHSI pumps for RHR function.	• LCO 3.3.1, Table 3.3.1-1, requires SI manual actuation only in MODES 1-4, does not require an engineered safety features actuation system (ESFAS) signal based on low loop level in any MODE, and does not require a sensor for RCS loop level. • LCO 3.4.11 requires that miniflow lines be open for any MHSI pump capable of injecting into the RCS in MODE 4 (when pressure is less than the low temperature overpressure (LTOP) arming temperature), MODE 5, and MODE 6 (when the reactor vessel head is on).
The RHR connection will be automatically isolated in the event of a break outside of the containment, based on the safeguard building sump level and pressure sensors.	• Section 9.3.3 on equipment and floor drains mentions double sump level measurement in the safeguard buildings, but no indication of a sump level signal or automatic RHR isolation could be found in TS or elsewhere in the FSAR.
Spring-loaded safety relief valve, located at the RHR hot leg suction line, protects the SIS/RHRS against over-pressurization when in RHR mode.	• LCO 3.4.11 does not require RHR suction relief valves as an alternative to pressurizer safety relief valves or an RCS vent.

Design Feature Identified in Section 5.4.7.2.1	Apparent Treatment in Technical Specifications
Redundant hot leg level sensors that initiate RCS make-up when the RCS hot leg has reached low level.	• LCO 3.3.1, Table 3.3.1-1, does not require a sensor for RCS loop level.
During mid-loop operation, the RCS loop level is controlled by the CVCS low pressure reducing valve to ensure there is sufficient RCS water inventory for operation of the LHSI pumps in RHR mode.	• Section 7.7.2.3.13 describes RCS loop level limitation, which is classified as a “control system not important to safety” and is not referred to in either TS or Tier 1.
The reactor pressure vessel (RPV) water level is continually monitored during outage with a level sensor.	• LCO 3.3.1, Table 3.3.1-1, does not require a sensor for RPV water level. • Section 7.1.1.5.7 indicates that the RPV level measurement system uses three temperature sensors at different heights in the hot leg. However, LCO 3.3.1, Table 3.3.1-1, requires hot leg temperature sensors only in MODES 1-3. Cold leg temperature sensors are required in MODES 1-6.
Temperature sensors, located at the RCS hot legs, allow temperature measurement of each hot leg when in a reduced inventory condition.	• LCO 3.3.1, Table 3.3.1-1, requires hot leg temperature sensors only in MODES 1-3. Cold leg temperature sensors are required in MODES 1-6.

Response to Question 19-27:

The response to this question will be provided by May 30, 2008.

Question 19-28:

Section 19.1.3.4.3 states that MHSI is actuated on either low level in the RCS loops or LHSI/RHR pump low suction pressure. Low loop level is addressed by the previous question on TS coverage. However, no discussion of the low suction pressure actuation signal could be found elsewhere in the FSAR. Please provide additional information on this diverse MHSI actuation signal and discuss how the availability of the sensor and actuation signal is ensured during shutdown.

Response to Question 19-28:

The diverse MHSI actuation signal is not credited in the U.S. EPR PRA model. Section 19.1.3.4.3 will be deleted.

FSAR Impact:

FSAR, Tier 2, Section 19.1.3.4.3 will be deleted.

Question 19-29:

Table 19.1-102 is missing key U.S. EPR features that reduce shutdown risk and their disposition (e.g., Tier 2, Tier 1, TS, or emergency response guidelines). Please augment this table in the following areas of shutdown risk (the examples are not inclusive): (a) Key design features or structures, systems, and components (SSCs) that reduce the potential of reactor coolant diversion from the vessel through the RHR/CVCS systems (b) Key design features, if any, that automate the response to losses of RHR (c) Key design features, if any, that automate RCS injection following loss of RHR, reactor coolant diversions, and LOCAs (d) Key operator actions and key pieces of instrumentation that are needed to support the associated operator actions (e.g., operator opening a gravity injection flow path) (e) Key SSCs that need to be available at shutdown to provide an alternate decay heat removal path using low pressure makeup and primary pressure relief (f) Key SSCs that are needed to reduce fire risk at shutdown and validate fire risk estimates (e.g., capability of fire watches when fire barriers are not intact)

Response to Question 19-29:

The response to this question will be provided by May 30, 2008.

Question 19-30:

Please document the status of containment during cold shutdown (MODE 5) when the RCS is completely intact and how these assumptions will be met (e.g., TS, administrative controls). This explanation should include the status of the equipment and personnel hatches, penetrations for operating systems, and temporary instrument and electrical penetrations. This explanation should also describe the operator's ability to close containment should a core damage event occur.

Response to Question 19-30:

As stated in the basis for the U.S. EPR Containment Technical Specification 3.6.1, the containment is not required to be operable in mode 5. During mode 5, assumptions on the containment availability as modeled in the SD PRA are based on crediting administrative controls. These administrative controls will include operating procedures that will meet the guidance of NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management," as described in the response to Question 19-12.

As described in FSAR Section 19.1.2.4, the COL applicant's PRA is a living document subject to the applicant's PRA maintenance and upgrade program. The COL applicant's PRA will be reviewed against future administrative controls and updated as necessary so that assumptions on containment isolation remain valid.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-31:

Please document in the status of containment during cold shutdown (MODE 5) up to when the refueling cavity is flooded with an open RCS (mid-loop operation is a subset of this phase of shutdown) and how these assumptions will be met (e.g., TS, administrative controls). This explanation should include the status of the equipment and personnel hatches, penetrations for operating systems, and temporary electrical and instrument penetrations. This explanation should also describe the operator's ability to close containment before steaming through an open RCS makes containment conditions intolerable to the operator.

Response to Question 19-31:

The status of containment for mode 5 is discussed in the response to Question 19-30.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-32:

Please identify the probabilities assumed for containment isolation during all phases of MODE 5.

Response to Question 19-32:

MODE 5 corresponds to POS C in the shutdown PRA; this includes conditions with level in the pressurizer (CA) and at mid-loop (CB). For mode 5 the shutdown PRA uses the same model for containment status as the at power PRA. The conditional probabilities for containment isolation failure for mode 5 events can be found in FSAR Table 19.1-101, page 19.1-414, for Release Categories 201-205, inclusive.

As stated in the basis for the U.S. EPR Containment Technical Specification 3.6.1, the containment is not required to be operable in mode 5. During mode 5 containment availability as modeled in the PRA is based on administrative controls. These administrative controls will include operating procedures that will meet the guidance of NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management," as described in the response to Question 19-12.

As described in FSAR Section 19.1.2.4, the COL applicant's PRA is a living document subject to the applicant's PRA maintenance and upgrade program. The COL applicant's PRA will be reviewed against future administrative controls and updated as necessary so that assumptions on containment isolation remain valid.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-33:

Please provide a complete electrical dependency matrix including all major accident mitigating systems to supplement Figure 19.1-3. This figure does not include, for example, electrical dependencies of the severe accident heat removal system (SAHRS).

Response to Question 19-33:

A response to this question will be provided by May 30, 2008.

Question 19-34:

The list of major modeling assumptions in Section 19.1.4.1.2.5 states that breaks are always assumed to occur in Train 4. However, the large break loss-of-coolant analysis in Chapter 15 appears to assume that the break occurs in Train 3 (see Table 15.6-8). Please discuss whether this difference in assumptions has any impact on the PRA results and insights.

Response to Question 19-34:

Assumption differences arise between the different analyses because the purpose of each analysis is different and demands its own set of assumptions in order to produce conservative results.

The PRA assumes loss of coolant breaks occur in Loop 4 because it produces more conservative PRA results due to plant configuration considerations. For example, the running CCW pump is associated with Train 4 and is assumed failed due to the break. This necessitates reliance on the starting of the standby pump(s) with an attendant start failure probability.

In the case of the Chapter 15 large break loss-of-coolant analysis, the worst break location (with respect to 10 CFR 50.46 criteria) is in the cold leg piping between the reactor coolant pump and the reactor vessel for the RCS loop containing the pressurizer. In the case of the U.S. EPR, the pressurizer is connected to the hot leg of Loop 3.

For small and medium sized breaks, the PRA assumption is consistent with the location assumption presented in Section 15.6.5.2.2, where small and medium size breaks are assumed to occur in the cold leg of Loop 4. Loop 4 was selected as a more limiting location with respect to RCP loop seal clearing.

The difference in assumptions arising from the large break loop selection will not impact LLOCA success criteria and therefore will not have an impact on the PRA results and insights.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-35:

Please describe how the treatment of induced steam generator tube ruptures, as described on page 19.1-22, considers the potential for multiple tube ruptures.

Response to Question 19-35:

As stated on FSAR page 19.1-22, the U.S. EPR PRA considers induced steam generator tube rupture (SGTR) as a separate initiating event. The frequency of this initiating event is calculated based on the method presented in NUREG/CR-6365 that considers single and multiple induced tubes ruptures. It references NUREG-0844, which gives the conditional probability, given an induced SGTR event, of rupturing a certain number of tubes, as follows:

- 1 tube: 0.49,
- 2 to 10 tubes: 0.5,
- More than 10 tubes: 0.01.

Given the SG tube material (Alloy 690) in this evaluation, rupture of 10 and more tubes is not considered. Probability to rupture one tube versus multiple tubes (less than 10) is considered equal. To summarize, the potential for multiple tube ruptures is considered as follow:

- 1 tube: 0.5,
- 2 to 10 tubes: 0.5.

The plant response is evaluated (through a simplified ISGTR event tree) to envelope the plant response to one and nine tube ruptures.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-36:

Please clarify whether the loss of a single switchgear, said on page 19.1-23 to "bound electrical failures," bounds alternating current (ac) failures only or both ac and direct current (dc) failures. If only ac failures are bounded, please discuss how the risk from dc bus failures is addressed, given that Table 19.1-3 states that the loss of a vital dc bus is not modeled.

Response to Question 19-36:

The loss of a single switchgear IE (31BDA) bounds only AC electrical failures; it is assumed to envelop a loss of three 6.9KV AC switchgears all in one division (Division 1). DC failures are not included. In the U.S. EPR design safety and non-safety busses are separated; therefore this initiating event includes losses of safety AC switchgears only. Neither AC loss nor DC loss of one division is likely to lead to an initiating event (automatic plant trip). A loss of one AC division was selected because it is more likely to challenge normal plant operation: Loss of Division 1 AC is assumed to fail the running CCW train, a CCW switchover would be required, and if not successful it would result in a loss of CCW Common Header 1 and a loss of cooling to two RCPs. It would also lead to a loss of the running charging pump and switchover will also be required. Moreover, the loss of AC division would eventually cause a loss of DC after the battery discharge time of two hours. A loss of DC bus is unlikely to result in an IE because it does not affect normally operating equipment. A simultaneous loss of AC/DC divisions is very unlikely without a significant spatial impact which is analyzed for the internal hazards.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-37:

Please clarify why HVAC recovery times “are expected to be site-specific,” as stated on page 19.1-23, rather than design-specific. For example, are different procedures, training, or plant layouts expected among sites?

Response to Question 19-37:

HVAC recovery times can be site-specific because of the different maximum ambient temperatures on the specific site. No PRA assumptions are made on the procedures, training, or plant layouts. Procedures, training and plant layouts are expected to be the similar at all U.S. EPR plants.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-38:

COL information item 19.1-9 states that the COL applicant must confirm that assumptions used in the PRA remain valid. Several areas for which the modeling is not complete or for which assumptions have been made (such as HVAC recovery times, instrumentation and controls (I&C) details, calibration errors, station blackout human errors, CVCS supply availability, and cooldown operator actions) are in different locations in Chapter 19. Please describe the strategy for communicating these assumptions to the COL applicants (e.g., collection of all assumptions in a single area in the PRA documentation).

Response to Question 19-38:

The response to this question will be provided by May 30, 2008.

Question 19-39:

Please provide additional information on the EFW pressure boundary conditions (EFW PBF) top event. The event tree success criterion is that four of four EFW storage pools maintain integrity, but Chapter 10 and TS appear to indicate that three pools or a minimum of 300,000 gallons are necessary for success.

Response to Question 19-39:

EFW PBF top event success criteria requires that four of four EFW storage pools maintain integrity because valves in EFW tanks crossties are normally open and a leakage in any EFW tank may disable them all, if not isolated on time with make-up being provided from demineralized water system.

A deterministic analysis provided in Chapter 10 and success criteria in the PRA are based on different requirements, and assumptions (for example PRA assumes a mission time of 24 hours for all systems), therefore the conclusions are not always identical.

FSAR Impact:

The FSAR will not be changed as a result of this question

Question 19-40:

Please provide additional detail on the “high-level review” for inter-system common-cause failures, as stated on page 19.1-41. Are there any cases in which the same parts (such as valves or pumps) are expected to be used in different systems? If so, how is the potential for common manufacturing defects or other common-cause failures removed?

Response to Question 19-40:

This high-level review for inter-system common-cause failures established the following:

1. Hardware–based, common-cause conditions (e.g., design, manufacturing and installation) between different systems are identified when the hardware is selected.
2. Operational conditions (function, procedures, maintenance/test/calibration) between different systems are likely to be different (different functions, different operating staff, staggered test, etc.).
3. Environmental conditions (component locations and environment, working mediums) between different systems are likely to be different (good spatial separation between trains and systems).

Based on the above, without component specific design and manufacturing information, there is no basis to include inter-system common-cause failures in the U.S. EPR PRA.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-41:

Please provide additional information on the full-load-rejection capability of the U.S. EPR and the planned actions following a LOOP. Page 19.1-12 states that the "design includes the capability to withstand a full load rejection without tripping the reactor" and that the design reduces "the potential for reactor trip and challenge to onsite emergency power systems for grid-centered [LOOP] events." However, page 19.1-23 states that a LOOP event results in a unit trip and affects mitigation response by placing demands on the onsite power system. If the LOOP event includes only events for which a reactor trip must occur, please discuss how the LOOP frequency was modified to account for this condition and how full-load rejection and a subsequent partial trip (as discussed on page 7.7-12) is modeled.

Response to Question 19-41:

The U.S. EPR is designed such that it can accept a 100 percent or less load rejection without a reactor or turbine trip. This design feature allows the plant to continue stable operation while the main generator supplies plant loads. Load rejection is accomplished by tripping the circuit breakers that connect the transmission lines to the switchyard, therefore separating the plant from the utility grid during a loss of the transmission system. During a load rejection, the connection from the main generator to the auxiliary transformers via the main step-up transformers and switchyard remains closed, maintaining plant loads energized.

During a LOOP event, power is lost from the switchyard to the station safety-related and non-safety-related busses (e.g., loss of the transmission system and failure of the load rejection). Following the LOOP, the planned actions and response are in accordance with operating procedures.

As modeled in the PRA, offsite power may be lost due to any of four groups of events: plant-centered faults, switchyard-centered faults, grid-related losses, and weather-related losses. Since the U.S. EPR 100% load rejection design requires the switchyard to be operational, only the grid related events are significantly reduced in severity as a result of this feature.

The LOOP Initiating Event Frequency was estimated as 1.91E-02 per reactor critical year based on NUREG/CR-6890. The NUREG/CR-6890 analysis was modified to remove the consequential (internal plant transient related) LOOP events (which are specifically modeled in the U.S. EPR model) and also to account for the full load rejection capability of the U.S. EPR design.

The probability that the full load rejection feature fails to operate as designed for a grid-related loss of offsite power event was estimated as 0.32 based on page A.A-17 of the Advanced Light Water Reactor Utility Requirements Document, Volume II ALWR Evolutionary Plant, May 1977.

The LOOP Initiating Event Frequency is estimated as 1.91E-02 events per reactor critical year. The calculation is summarized in Table 19-41-1.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Table 19-41-1—Calculation of the U.S. EPR LOOP Initiating Event Frequency

LOOP Initiating Event	# LOOP Initiating Events (1997 - 2004)	# CNSQ LOOP Events (1997 - 2004)	IEF (prcy) NUREG/CR-6890 [3]	IEF (prcy) Excluding consequential LOOPs[1]	U.S. EPR LOOP IEF[2]
Plant Centered	1	0	2.07E-03	2.07E-03	2.07E-03
Switchyard Centered	4	3	1.04E-02	6.21E-03	6.21E-03
Grid Related	13	0	1.86E-02	1.86E-02	5.96E-03
Weather Related	3	0	4.83E-03	4.83E-03	4.83E-03
Total			3.59E-02	3.18E-02	**1.91E-02**

1. Since consequential loss of offsite power events are specifically modeled in the systems analysis they are excluded from the Initiating Events analysis.
2. The U.S. EPR LOOP IEF excludes consequential LOOPs and accounts for the impact of the full load rejection capability. The LOOP IEF frequency due to grid related events is reduced to account for the fact that the full-load rejection feature is estimated to prevent a reactor trip for 68% of grid related loss of offsite power events.
3. The IEF is calculated using the NUREG/CR-6890 Volume 1 approach. The mean is a Bayesian update using a Jeffreys prior. Mean = (0.5 + events)/(critical or shutdown years). This is the NUREG/CR-6890 result, including consequential LOOP events, and not accounting for the full load rejection capability of the U.S. EPR design.

Question 19-42:

Please clarify the first bullet on page 19.1-57 on the difference in modeling CCW and ESW losses between the system fault trees and the initiating event models. Why was a loss of a CCW train assumed to cause a loss of the corresponding ESW train in the initiating events model?

Response to Question 19-42:

CCW and ESW losses are modeled as:

1. *Loss of support to the main mitigating systems in the event trees:* The separate system fault trees are developed for the CCW and ESW trains. These systems are support systems for many safety functions credited in the PRA (EDG cooling, seal injection and cooling, safety injection, etc.). In all but one of these functions, cooling is provided by CCW trains, which are cooled by corresponding ESW trains. Only EDG cooling is provided directly by ESW.
2. *Initiating events:* Losses of CCW common headers (1 or 2) are modeled as multiple initiators (eight different combinations). These losses could occur either because of failures in the CCW trains, or failures in the corresponding ESW trains. These trains are separately modeled in the CCW IE fault trees. However, in order to simplify the model no separate IEs are modeled for the losses of ESW only. The separate modeling would result in eight additional initiating events, with almost the same effects (loss of CCW common header and loss of cooling to safety injection pumps). The effect which would not be the same is “a loss of cooling to EDGs”. If a specific CCW IE occurs because of the failures in the CCW system only, cooling to the EDGs may still be available from the ESW. However, in order to significantly reduce the number of modeled IEs, it was conservatively assumed that a loss of CCW train in the CCW IE model implies that the corresponding ESW train is also unavailable. For example, for IE LOCCW1, which models a loss CCW CH1, due to of a CCW Train 1 failure and an unsuccessful switchover to CCW Train 2, the following trains are all assumed disabled: CCW CH1, CCW Train 1 and ESW Train 1.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-43:

Please provide additional information on what types of electrical interdependencies between HVAC divisions may not be included in the model, as mentioned on page 19.1 57. What effect is this omission expected to have on the overall risk insights and conclusions?

Response to Question 19-43:

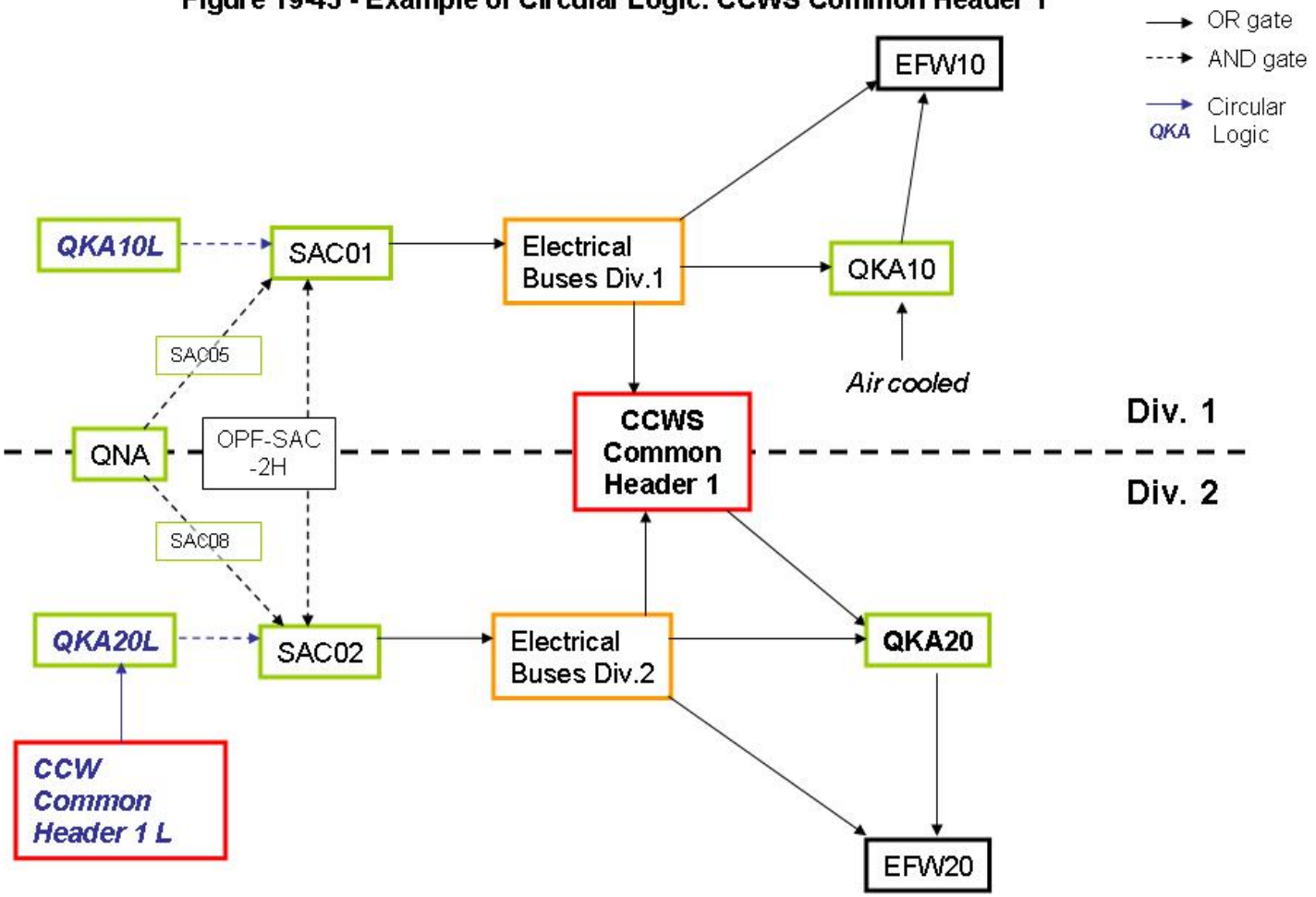
HVAC system supports the operation of the electrical busses (switchgear room ventilation); therefore, to avoid circular logic, fault trees for all systems that directly and indirectly support HVAC operation are replaced by their circular logic equivalents (no power supplies). Because of this circular logic, the resulting fault trees, under certain failure combinations, may not handle interdependencies between two HVAC divisions properly. For example, a loss of HVAC Train 1, if possible recoveries are not successful, could result in a loss of a running CCW train. This in turn would degrade the switchover ability, resulting in a loss of CCW common header 1, and, if HVAC maintenance trains are not available, in a loss of cooling to HVAC Train 2.

Because of the circular logic, the above interdependency will not show directly in the PRA results. The total impact is expected to be small because HVAC Train 2 cooling to the EFW room properly captures this dependency, so that EFW Train 2 would be lost (one of the most important mitigating trains). The circular logic is illustrated in Figure 19-43 - Example of Circular Logic: CCWS Common Header 1.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Figure 19-43 - Example of Circular Logic: CCWS Common Header 1



Question 19-44:

Please clarify the statement on page 19.1-58 that "some simplifying assumptions are used for the inter-dependent support systems." Does this statement refer to the removal of circular logic, or have additional assumptions been made? What is the overall effect on the risk insights and conclusions?

Response to Question 19-44:

The above statement does not refer to a circular logic issue, but to modeling assumptions made on the running support systems, which make the plant PRA model asymmetric. This refers to the following type of assumptions:

- LOCA breaks occur in Train 4.
- CCW/ESW Train 1 & 4 are running trains, feeding CH1 & CH2, etc.

The overall effect on the risk insights is small. Importance measures may yield asymmetrical results for differential timing; however, insights on the relative importance would not be affected (the train with the highest importance would be considered to represent the system.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Question 19-45:

Please clarify the statement on page 19.1-58 that an electrical realignment of the main steam relief isolation valves (MSRIVs) would cause a 16 percent improvement in the CDF. Table 19.1-15 appears to indicate a 7% decrease in CDF for this case. Additionally, please discuss other design changes that were considered to potentially improve risk; this MSRIV change appears to be the only change included in Table 19.1-15.

Response to Question 19-45:

The statement on page 19.1-58 indicating that an electrical realignment of the MSRIVs would cause "a 16 percent improvement" in the CDF has a typo, and it should read "a 7 percent improvement". FSAR Table 19.1-15 is correct.

Through the history of the EPR design development, many design changes have already been made based on the PRA insights. These are discussed in Section 19.1.3.4. Design decisions in U.S. EPR development are evaluated by the PRA group. Other than the MSRIVs realignment, no other significant improvements have been identified in this phase. Other design changes that were considered (but not documented in the FSAR) are given below:

1. Isolating fire water from the annulus.
2. Keeping EFW suction crossties closed.
3. Using different logic for the CCW switchover.

FSAR Impact:

FSAR, Tier 2, page 19.1-58 will be revised to correct the typographical error described in the response to the question.

Question 19-46:

Please provide additional detail on the modeling uncertainty cases discussed on page 19.1-59 and 19.1-60. How was the probability of each success criterion derived? How is the subsequent weighted average modeled?

Response to Question 19-46:

The modeling uncertainty cases are defined below:

CASE 1a, Number of EFW pumps required for SHR success in the case of LoMFW:

- Case 1 of 4: probability 0.3.
- Case 2 of 4: probability 0.5.
- Case 3 of 4: probability 0.15.
- Case 4 of 4: probability 0.05.

Case 1b, Number of EFW pumps required for SHR success in the case of LOOP (RCP tripped):

- Case 1 of 4: probability 0.5.
- Case 2 of 4: probability 0.3.
- Case 3 of 4: probability 0.2.

Case 2, Number of Pressurizer Safety Valves (PSV) required for Feed and Bleed success:

- Case 1 of 3: probability 0.1.
- Case 2 of 3: probability 0.4.
- Case 3 of 3: probability 0.5.

Case 3, Success criteria for the second recovery of the HVAC system for the SWGR rooms for one division:

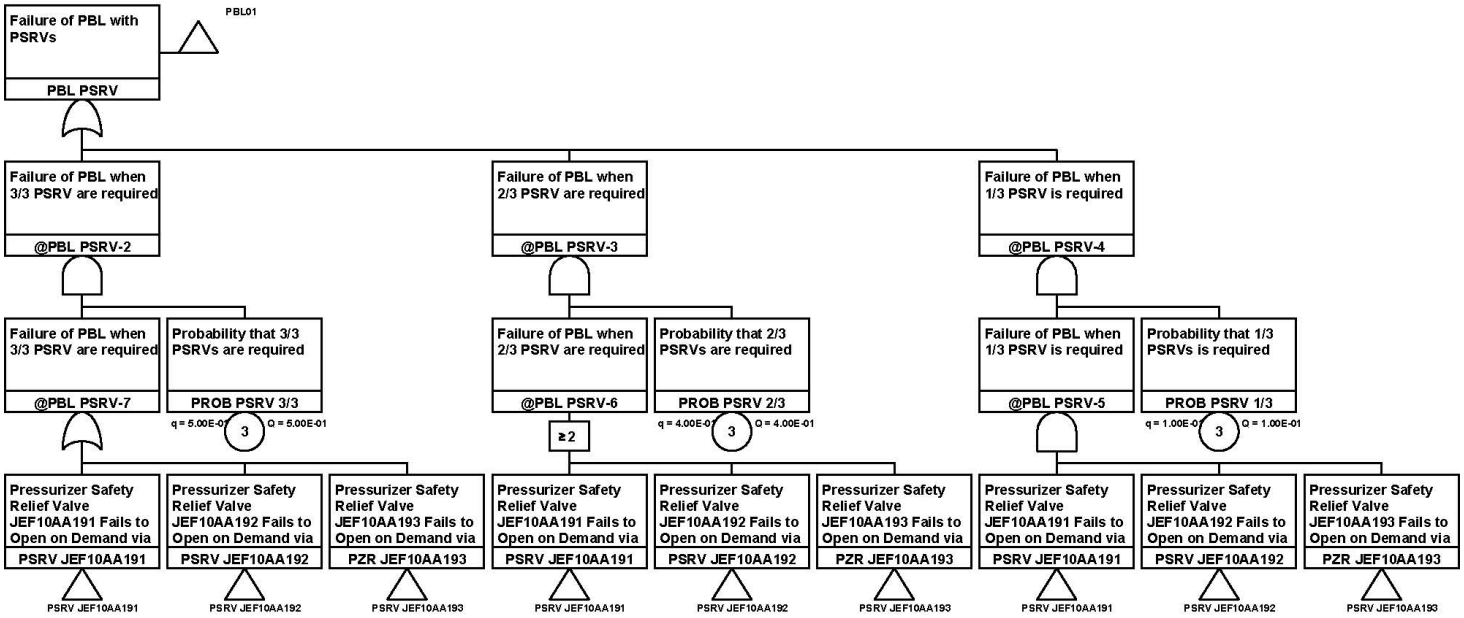
- No recovery is required: probability 0.05.
- Recovery required in four hours: probability 0.4.
- Recovery required in two hours: probability 0.5.
- Recovery not possible: probability of 0.05.

These cases are selected in order to identify possible uncertainties in the success criteria; they are based on the differences in the success criteria observed in global EPR PRAs. Corresponding probabilities are assigned based on engineering judgment. The different success criteria and corresponding probabilities are entered directly in the fault trees, as illustrated in Figure 19-46 – Example of Fault Tree Used to Evaluate Modeling Uncertainty. Therefore, the modified Risk Spectrum run has provided the weighted average.

FSAR Impact:

The FSAR will not be changed as a result of this question.

Figure 19-46 - Example of Fault Tree Used to Evaluate Modeling Uncertainty



PBL PSRV