SCIE-NRC-239-95

FORT CALHOUN UNIT 1
TECHNICAL EVALUATION REPORT
ON THE INDIVIDUAL PLANT EXAMINATION
BACK-END ANALYSIS

H. A. Wagage
J. F. Meyer

Prepared for the U.S. Nuclear Regulatory Commission
Under Contract NRC-04-91-068-40
May 1996

SCIENTECH, Inc.
11140 Rockville Pike, Suite 500
Rockville, Maryland 20852

TABLE OF CONTENTS

E. EXECUTIVE SUMMARY

E.1 Plant Characterization

The Fort Calhoun Station (FCS) consists of a Combustion Engineering nuclear steam supply system (NSSS) with a General Electric turbine. Gibbs and Hill designed the balance of the plant and the auxiliary systems.

The reactor system consists of a pressurized water reactor and its associated coolant system arranged as two closed loops, each containing two reactor coolant pumps and a steam generator connected in parallel to the reactor. An electrically heated pressurizer is connected to one of the loops. The system is designed to operate at a core thermal power of 1500 MWt to provide steam at 850 psia.

The containment building consists of a concrete structure in the form of a vertical cylinder with domed roof and a flat base. The cylinder and dome are made of post-tensioned concrete and the base is made of reinforced concrete construction. A continuous carbon steel liner is included. Inside the containment structure, the reactor and other NSSS components are shielded with concrete. Facilities are provided for pressure and leak rate testing of the entire containment system.

The FCS containment was designed by Gibbs and Hill and has an internal free volume of 1.05 million cubic feet. The containment has a design pressure rating of 60 psig and a median ultimate pressure of 215 psig. This ultimate pressure is higher than that calculated for most of the other plants and therefore the Fort Calhoun containment is likely to outperform many other containments in the event of a hydrogen burn.

E.2 Licensee's IPE Process

The IPE team performed a level III probabilistic risk analysis (PRA) for the FCS IPE. The IPE team developed containment event trees (CETs) and supporting logic models similar to fault trees to interface with the level I plant damage states. The team determined the behavior of containment by various walkdowns, training, and literature reviews about core melt phenomena. The team performed Modular Accident Analysis Program (MAAP) computer code runs to obtain more specific information about phenomena timing and parameters such as pressures and temperatures of specific core melt scenarios. MAAP also produced radioisotope information for input into level III analysis.

The FCS level II analysis consisted of the following major tasks: containment event trees, link level-I analysis with level-II analysis, containment ultimate structural analysis, plant walkdowns, and MAAP runs.

Omaha Public Power District (OPPD) provided the overall technical management of the FCS IPE. The IPE program was run by the Supervisor of System Analysis, who reported to the Manager of Nuclear Design Engineering. SAIC provided consulting service to the project at the beginning, and Combustion Engineering added plant-specific information later in the project. Other contractors with specialized skills were also used (not listed in the submittal).

As the project progressed, more work was increasingly done in-house, with consultants used in areas of special expertise. In-house expertise with the design engineering group was used in the areas of structural, electrical, and thermohydraulics engineering. The submittal notes that well over 50 % of the total engineering effort applied to the project had been contributed by OPPD personnel.

There were three levels of review of the IPE submittal. For example, during the first level of review, a PRA Oversight Committee composed of OPPD personnel from System Engineering, Licensing, Training, Operations, Civil Engineering, Electrical Engineering, and Mechanical Engineering met with the PRA group every two weeks to discuss the IPE results in general and specific findings.

E.3 Back-End Analysis

The IPE team used CETs to quantify containment failure modes and the radionuclide releases. The containment failure modes and the major phenomena that have a significant impact on the radionuclide release fractions were represented as top events on the CET. Detailed evaluations of phenomena which affected containment failure timing, fission product releases, or which may have an impact on downstream top events were treated by using supporting logic models. This approach allowed a relatively detailed treatment of the phenomena affecting containment performance while maintaining a relatively simple CET. Also, each end point on the CET represented a distinct release class. The CET used plant damage states (PDSs) as input.

Because the release consequences were affected by core melt timing and since there were differences in the various severe accident progressions, separate CETs were developed for the different core melt timing conditions - early, delayed, and late.

The IPE team defined early containment failure as occurring either at or within one hour of reactor vessel failure. They defined late containment failure as occurring later than one hour of reactor vessel failure.

Overall, the containment remained intact 59.8 % of the time following a severe accident. Consequently the containment failed 40.2 % of the time for these sequences. The percentage of intact containment without accompanied vessel breach occurring was 26.0 %.

The following were the contributions for 40.2 % of the containment failures (alpha mode failure and basemat melt-through failures were negligible):

- Late containment failure 28.0 %
- Bypass (interfacing systems LOCAs - 4.9 % and SGTR - 0.5 %) 5.4 %
- Containment isolation failure 5.1 %
  (isolation valve failure - 0.13 % and SGTR* - 5.0 %)
- Early containment failure 1.6 %

(* In other IPE submittals, the SGTR-event is completely grouped in bypass.)

E.4 Generic and Containment Performance Improvement Issues

As a result of the Containment Performance Improvement (CPI) program, recommendations were made for consideration by licensees as part of the IPE process. These recommendations were identified in Generic Letter 88-20, Supplement 3. The recommendation applicable to the FCS is as follows:

> Licensees with dry containments are expected to evaluate containment and equipment vulnerabilities to localized hydrogen combustion and the need for improvements (including accident management procedures) as part of the IPE.

In response to the NRC staff's RAI, the licensee notes the following:

> The containment structure was walked down and prints were reviewed to determine if there were hydrogen "pockets" where hydrogen could cause equipment needed for accident mitigation to be damaged. No vulnerabilities were found, i.e., no pockets were found where damage to equipment would occur.

E.5 Vulnerabilities and Plant Improvements

The licensee response to the NRC staff's RAI provides the following information. The IPE team retained all the sequences that met the guidelines in NUMARC 91-04. In performing the containment performance analyses, the IPE team coupled all retained core damage sequences with the containment safeguards sequences to generate plant accident sequences (PASs). They mapped all PASs with a frequency of greater than or equal to 1E-9, or which covered potential vulnerabilities, into PDSs. They mapped all PDSs into release classes by being propagated through the CET. The IPE team used all release classes with frequency greater than 5E-10 in the calculation of risk. The IPE team reviewed the retained release classes for potential containment vulnerabilities. They found no severe accident vulnerabilities unique to the plant.

The plant improvements related to the IPE involved with the front-end analysis.

E.6 Observations

The FCS IPE submittal contains a substantial amount of information with regard to the recommendations of GL 88-20, its supplements, and NUREG-1335. The submittal appears to be complete in accordance with the level of detail requested in NUREG-1335. The methodology used to perform the IPE is described clearly in the submittal. The approach taken, which is consistent with the basic tenets of GL 88-20, Appendix 1, is also described clearly along with the team's basic underlying assumptions. The important plant information and data are well documented and the key IPE results and findings are well presented.

The IPE team found no severe accident vulnerabilities unique to the FCS. They identified no back-end plant improvements.

1. INTRODUCTION

1.1 Review Process

This technical evaluation report (TER) documents the results of the SCIENTECH review of the back-end portion of the Fort Calhoun Station Unit 1 (FCS) Individual Plant Examination (IPE) submittal [1, 2]. This technical evaluation report complies with the requirements for reviews of the U.S. Nuclear Regulatory Commission (NRC) contractor task order, and adopts the NRC review objectives, which include the following:

- To help NRC staff determine if the IPE submittal provides the level of detail requested in the "Submittal Guidance Document," NUREG-1335
- To help NRC staff assess the strengths and the weaknesses of the IPE submittal
- To complete the IPE Evaluation Data Summary Sheet

Based in part on SCIENTECH's preliminary review of the Callaway IPE submittal, the NRC staff submitted a Request for Additional Information (RAI) to the Omaha Public Power District on September 12, 1995. The Omaha Public Power District responded to the RAI in a document dated November 30, 1995. [2] This final TER is based on the original submittal and the response to the RAI.

Section 2 of the TER summarizes our review findings and briefly describes the FCS IPE submittal as it pertains to the work requirements outlined in the contractor task order. Each portion of section 2 corresponds to a specific work requirement. Section 3 presents our overall evaluation of the back-end portion of the FCS IPE based on our submittal-only review. Section 3 also outlines the conclusions and insights gained, plant improvements identified, and utility commitments made as a result of the IPE. References are given in section 4. Appendix contains an IPE evaluation and data summary sheet.

1.2 Plant Characterization

The FCS consists of a Combustion Engineering nuclear steam supply system (NSSS) with a General Electric turbine. Gibbs and Hill designed the balance of the plant and the auxiliary systems.

The reactor system consists of a pressurized water reactor and its associated coolant system arranged as two closed loops, each containing two reactor coolant pumps and a steam generator connected in parallel to the reactor. An electrically heated pressurizer is connected to one of the loops. The system is designed to operate at a core thermal power of 1500 MWt to provide steam at 850 psia.

The containment building consists of a concrete structure in the form of a vertical cylinder with domed roof and a flat base. The cylinder and dome are made of post-tensioned concrete and the base is made of reinforced concrete construction. A continuous carbon steel liner is included. Inside the containment structure, the reactor and other NSSS components are shielded with concrete. Facilities are provided for pressure and leak rate testing of the entire containment system.

The FCS containment was designed by Gibbs and Hill and has an internal free volume of 1.05 million cubic feet. The containment has a design pressure rating of 60 psig and a median ultimate pressure of 215 psig.

The containment has an inside diameter of 110 feet with an inside height of 137.4 feet. The foundation slab is 13 feet thick. The side walls are 3.875 feet thick and the domed roof is 3 feet thick. The walls and roof have 616 and 210 imbedded post-tensioned cables respectively. These cables provide external force to the structure to compensate for internal forces that occur during a design basis accident (DBA).

The concrete foundation mat is constructed from a 50/50 limestone/common sand mixture and is reinforced with high strength reinforcing steel. A permanent access gallery extends under the containment structure directly below the cylindrical wall.

The containment has a maximum leak rate of 0.1 weight percent of containment atmosphere over a 24-hour period at 60 psig and 305 °F after a DBA.

Items of particular note in the FCS design from a containment performance (level II) and radiological consequence (level III) perspective include (section 4.1.1, page 4.1-1):

- A "passively" flooded reactor cavity combined with an integral "instrument-free" lower head which enables "in-vessel" retention of corium debris via external vessel cooling.

- A robust containment and reactor cavity design which reduces the contribution of early containment failure to less than 2 % of all core damage sequences.

- A large basemat area to promote spreading of the corium melt following vessel breach and ex-vessel cooling of corium debris when an overlying water pool is present.

- A very thick basemat which prolongs the time to containment failure associated with corium basemat erosion.

2. TECHNICAL REVIEW

In performing the "submittal only" review, SCIENTECH compared the FCS IPE submittal with the recommendations of Generic Letter (GL) 88-20 and its supplements, according to the guidance provided in NUREG-1335. We used the structure of Task Order Subtask 1 in setting out the review findings reported in this section which addresses the key points of the GL and its supplements. This TER also notes inconsistencies between the FCS IPE and other PRA studies in terms of the methodology used and results obtained and identifies the FCS IPE strengths and weaknesses.

2.1 Licensee's IPE Process

2.1.1 Completeness and Methodology.

The FCS IPE submittal contains a substantial amount of information with regard to the recommendations of GL 88-20, its supplements, and NUREG-1335. The submittal appears to be complete in accordance with the level of detail requested in NUREG-1335. The methodology used to perform the IPE is described clearly in the submittal. The approach taken, which is consistent with the basic tenets of GL 88-20, Appendix 1, is also described clearly along with the team's basic underlying assumptions. The important plant information and data are well documented and the key IPE results and findings are well presented.

The IPE team performed a level III probabilistic risk analysis (PRA) for the FCS IPE. The IPE team developed containment event trees (CETs) and supporting logic models similar to fault trees to interface with the level I plant damage states. The team determined the behavior of containment by various walkdowns, training, and literature reviews about core melt phenomena. The team performed Modular Accident Analysis Program (MAAP) computer code runs to obtain more specific information about phenomena timing and parameters such as pressures and temperatures of specific core melt scenarios. MAAP also produced radioisotope information for input into level III analysis.

The FCS level II analysis consisted of the following major tasks:

- Containment Event Trees. Develop CETs depicting possible accident progression after core damage that are phenomena-based, and quantify the events using supporting logic models.

- Link Level-I Analysis with Level-II Analysis. Using plant damage states (PDSs) and plant damage bins, link the level I core damage states to the CETs.

- Containment Ultimate Structural Analysis. Use finite element analysis to determine the limiting conditions that various containment components and structures will withstand before failure.

- Plant Walkdowns. Observe and become familiar with the layout in containment and the auxiliary building including key component and structure locations to comprehensively understand how various phenomena will affect the components and structures and to define release paths to the environment.

- MAAP Runs. Run scenarios that cover the range of severe accidents so that timing of events, magnitude of events, and parameters of the accidents can be estimated.

2.1.2 Multi-Unit Effects and As-Built/As-Operated Status.

Multi-unit effects are not applicable to FCS because it is a single unit site.

To ensure as-built, as-operated modeling of FCS, the IPE team undertook several data collection and documentation activities during the initial phase of the project. The IPE team performed plant walkdowns during which the team observed and became familiar with the layout in containment and the auxiliary building including key component and structure locations to comprehensively understand how various phenomena will affect the components and structures and to define release paths to the environment. The team prepared system notebooks after plant walkdowns and reviews of drawings, system descriptions, the Updated Safety Analysis Report, Technical Specifications, and applicable plant procedures.

2.1.3 Licensee Participation and Peer Review.

Omaha Public Power District (OPPD) provided the overall technical management of the FCS IPE. The IPE program was run by the Supervisor of System Analysis, who reported to the Manager of Nuclear Design Engineering. SAIC provided consulting service to the project at the beginning, and Combustion Engineering added plant-specific information later in the project. Other contractors with specialized skills were also used (not listed in the submittal).

The development of the plant risk model involved "extensive interfacing/review with Production Engineering Division to understand the design of the plant, the operations personnel to fully understand the operating procedures, and the maintenance and reliability personnel to understand maintenance philosophy and scheduling." (section 5.1, page 5.0-2)

As the project progressed, more work was increasingly done in-house, with consultants used in areas of special expertise. In-house expertise with the design engineering group was used in the areas of structural, electrical, and thermohydraulics engineering. The submittal notes that well over 50 % of the total engineering effort applied to the project had been contributed by OPPD personnel (section 1.4, page 1.1-4).

There were three levels of review of the IPE submittal. For the first level of review, a PRA Oversight Committee composed of OPPD personnel from System Engineering, Licensing, Training, Operations, Civil Engineering, Electrical Engineering, and Mechanical Engineering met with the PRA group every two weeks to discuss the IPE results in general and specific findings.

The second level of review was performed by the PRA Executive Committee consisting of the Senior Vice President and the three nuclear Division Managers, along with selected department managers. This group reviewed and proposed resolution for the significant PRA findings.

The third level of the review was performed by a team organized by Duke Engineering and Services composed of experts in PRA from Duke Engineering, Yankee Atomic Electric Company, and ABB/Combustion Engineering. This team, composed of a total of five people experienced in PRA, peer reviewed the IPE to 1) ensure the accuracy of the documentation package and to validate both the IPE process and its results and 2) determine whether the analysis methods used met the intent of GL 88-20.

The comments were mostly general on the IPE program or on the level I analysis.

2.2 Containment Analysis

2.2.1 Front-end Back-end Dependencies.

The IPE team defined the FCS PDSs based on eight characteristics as given in table 1. By using the ORACLE data base system [3] and all the possible combinations of these characteristics, the team defined 9,072 PDSs. A set of deletion rules was developed to delete combinations which were physically impossible or were counter to other definitions used in the analysis. By excluding physically impossible combinations of characteristics, the IPE team reduced the number of PDSs to be considered to 510.

The IPE team evaluated containment safeguards (CSG) using a CSG event tree. Several branches of this event tree were evaluated using CAFTA computer code. A fault tree linking approach was used to solve the CSG event tree and create the CSG states. The cutsets in the CSG states were combined with the core damage cutsets using COMBINE code. The resultant cutsets were referred to as plant accident sequences (PASs). The final PAS cutsets were produced by deleting success path cutsets and mutually exclusive cutsets as appropriate.

Table 1. FCS Plant Damage State Parameters

No.	Parameter	Parameter Value	Code
1.	RCS pressure	High (> 1200 psia)	HIGH
		Medium (between 250 psia and 1200 psia)	MED
		Low (< 250 psia)	LOW
2.	RCS leak rate	Large LOCA	LL
		Medium LOCA	ML
		Small LOCA	SL
		SGTR	SGTR
		Cycling relief valve/PORV	CRV
		Intersystem LOCA (large)	ISLL
		Intersystem LOCA (small)	ISLS
3.	Steam generator availability	Available	SGA
		Unavailable	SGU
		Status not applicable	SGNA
4.	Core melt timing	Early (< 2 hours)	EARLY
		Delayed (2 to 6 hours)	DELAY
		Late (> 6 hours)	LATE
5.	Containment spray system availability	Available in both injection and recirculation modes	CSA
		Available in injection mode but not in recirculation mode	CSI
		Unavailable	CSU
6.	Containment heat removal availability	Available (containment air recirculation cooling and/or containment spray heat exchangers available)	CHA
		Unavailable	CHU
7.	Cavity condition	Dry (no water)	DRY
		Low flood (wet below reactor vessel only)	LOW
		Medium flood (wet to top of RV lower head)	MID
		Full flood (wet to top of active fuel)	FULl
8.	Containment isolation	Isolated	CI
		Not isolated	CNI

Each PAS cutset was inspected and assigned to a PDS. Leak rate, steam generator status, and containment safeguards status were specified directly by the PASs. Core melt timing and cavity status were inferred on a cutset-by-cutset basis using knowledge of the core damage and CSG sequences.

The quantified PDSs were filtered based on a cutoff value of 1E-9. PDSs that were considered to be important (e.g., interfacing system LOCAs) were retained, although they

were below the cutoff value. The resultant list consisting of 45 PDSs represented the dominant PDSs which were analyzed in the level II PRA.

The process used by the IPE team to define PDSs to be analyzed in the level II PRA appears to have been complete in accounting for the front-end back-end dependencies of accident progression.

2.2.2 Containment Event Tree Development.

The IPE team used CETs to quantify containment failure modes and the radionuclide releases. The containment failure modes and the major phenomena that have a significant impact on the radionuclide release fractions were represented as top events on the CET. Detailed evaluations of phenomena which affected containment failure timing, fission product releases, or which may have an impact on downstream top events were treated by using supporting logic models. This approach allowed a relatively detailed treatment of the phenomena affecting containment performance while maintaining a relatively simple CET. Also, each end point on the CET represented a distinct release class. The CET used PDSs as input.

Because the release consequences were affected by core melt timing and there were differences in the various severe accident progressions, separate CETs were developed for the different core melt timing conditions - early, delayed, and late. For convenience, the portions of the CETs pertaining to isolation failure and alpha failure were presented separately. This treatment resulted in a total of six CETs. Following were the 13 CET top events used:

- Is containment bypass presented?
- Is containment isolated?
- Is containment failure due to in-vessel steam explosion prevented?
- Is vessel breach prevented?
- Is early containment failure prevented?
- Is late containment failure prevented?
- Is basemat melt-through prevented?
- Is in-vessel fission product scrubbing available?
- Is a vaporization release prevented?
- Is a release prevented?
- Is a revaporization release scrubbed?
- Is a vaporization release scrubbed?
- Are intact containment fission products scrubbed?

The IPE team developed a supporting logic tree to further analyze each of the above top events, except the first two and the last one.

2.2.3 Containment Failure Modes and Timing.

Fragility curves, covering full range of pressures versus failure probabilities for the following potential failure modes, were developed for the FCS:

- Bending failure of basemat
- Shear failure of basemat
- Membrane failure of cylindrical shell
- Bending failure of the basemat-cylindrical shell juncture
- Shear failure of the basemat-cylindrical shell juncture
- Dome membrane failure
- Equipment hatch failure

Fragility curves were developed for 95 %, 50 % (median), and 5 % confidence levels for the above failure modes and their combinations. The team investigated the following four additional failure modes for which no fragility curves were developed:

- Personnel hatch failure
- Refueling penetration failure
- Mechanical penetration failure
- Electrical penetration failure

To evaluate the containment capacity when subjected to an overpressure load, Stevenson & Associates performed a finite element analysis using a global axisymmetric model. Local models were developed to evaluate the areas of the penetrations. Both static and dynamic analysis were performed using the ANSYS-PC/LINEAR code. [4] In the global finite element model, the presence of the internal structure on the basemat was considered in a simplified form. Because no detailed design information was available, the analysts assumed a distributed weight of 45,000 tons.

The dynamic overpressure calculation was performed by subjecting the axisymmetric model to a time evolution described by a triangular impulse decaying to a constant pressure value of 15 % of the peak pressure. The magnitude of this loading was generally analogous to a detonation shock wave pulse. The total duration of the triangular impulse was 0.01 seconds. To compute the fragility curves, the peak pressure level was varied from 60 psi to 600 psi.

The containment shell failure is dominated by three failure modes: 1) tension failure due to high membrane forces in the hoop direction in the cylinder above the mid-height, 2) tension failure in hoop/meridian direction due to high membrane forces in the dome at the center, and 3) shear failure due to shear forces at the base of the cylinder, near the joint with the basemat. The median failure pressures of the containment under these failure modes were calculated to be 235, 285, and 268 psig. The licensee response to the NRC staff's RAI notes that the median failure pressure of the CPS containment from all the modes was 215 psig.

The IPE team considered temperature induced failures of containment that result from high temperature degradation of NORDEL EPDM (ethylene-propylene type) seals used for all FCS penetrations (section 4.2.3.4.1, page 4.2-104). The team reviewed the FCS Updated Safety Analysis Report for the capabilities of the EPDM based sealants, and found that the mean instantaneous failure temperature of seal material was about 620 °F which was independent of the test environment media. Because that analyses of typical FCS accident scenarios showed that sustained temperatures in excess of 375°F were unlikely, instantaneous failure of seals were considered unlikely.

Temperature induced containment failure resulting from penetration sealant degradation was considered possible for all sequences where containment heat removal was lost and the reactor cavity was expected to be dry (i.e., occurrence of core concrete interactions). In evaluating radiological consequences of containment overtemperatures, the containment failure mode was assumed to be a small leak.

2.2.4 Containment Isolation Failure.

The IPE team considered that loss of containment isolation could occur directly as a result of the inability to isolate containment penetrations following a severe accident or indirectly as a result of a steam generator tube rupture (SGTR) with a consequent failure of secondary safety valves, atmospheric dump valves (ADVs), or turbine bypass valves.

Because SGTRs would result in successful isolation of the affected steam generator, most SGTRs (including those resulting in severe core damage) were considered to cause small environmental releases. Even if the affected steam generator was not isolated, secondary water that is available to the steam generator secondary side would produce a favorable environment (cool and low steaming rate) within the primary side of the steam generator tubes for fission products retention. When the secondary side water level covered the broken tube elevation, most iodine and cesium that leave the primary side would be scrubbed out in the secondary side water pool.

Within the PRA, SGTRs were considered bypass events only if the affected steam generator was not isolated. (Note that most of the other IPEs categorized SGTR as a containment bypass.) This situation would arise from the inability to depressurize the steam generator and result in a condition where the main steam safety valves (MSSVs) cycle, releasing radiation intermittently, or from transients where a MSSV or ADV is stuck open.

Isolation failure from inability to close containment isolation valves had a combined frequency of 1.7E-8 per year (0.13 % of the total CDF). The consequences of these events depended on the availability of containment heat removal and sprays during the sequences. Isolation failure associated with a SGTR had a total frequency of 6.8E-7 per year (5.0 % of the total CDF).

The IPE team found that loss of FCS containment isolation was highly unlikely, mainly because of the following preventive features in the FCS design (section 4.2.2.5.3):

- Use of double isolation valves for containment penetrations
- Use of diverse means of powering isolation valves
- Selection of isolation valve failure position consistent with its safety related function

2.2.5 System/Human Response.

The utility response to NRC staff's RAI notes that the IPE team conservatively assumed that the operators would not open the PORVs to depressurize the RCS because of lack of procedures (response 37, reference 2). The utility plans to incorporate guidance on PORV operation during severe core damage events into plant-specific accident management procedures.

The IPE team performed a sensitivity study to evaluate the impact of assuming a 50 % chance that the operators would open the PORVs to depressurize the RCS. This resulted in a slight increase in the frequency of the intact non-vessel breach sequences and a slight decrease in the frequency of early containment failures due to ex-vessel steam explosions.

There were five other operator recovery or mitigation actions that were included in the back-end analyses. These actions and the locations of their discussions in the submittal are listed in table 2 below.

2.2.6 Radionuclide Release Categories and Characterization.

As noted in section 2.2.2 of this report, the IPE team developed six CETs which addressed the various combinations of isolation status (failed/not failed), alpha failures, and core melt timing. The end states of these event trees defined a total of 201 potential

Table 2. Additional Operator Recovery or Mitigation Actions in Back-end Analyses

Action	Event Name	Location in Submittal [1]	
		Section	Page
Containment heat removal not recovered	NCHRECOV	4.6.7.1.2	4.6-36
Power is recovered late in the accident	RESPARK	4.6.7.1.10	4.6-39
High pressure ECCS recovered during core melt	SHP-SIS1	4.6.5.1.6	4.6-13
Low pressure ECCS recovered during core melt	SLP-SIS1	4.6.5.1.7	4.6-14
Containment sprays recovered	SPRAYRECOV	4.6.9.1.3	4.6-47

release states for each PDS. After quantifying the CETs, there were a total of 44 release classes with a non-zero frequency. This included 12 early core melt sequence release classes, 16 delayed core melt sequence release classes, and 16 late core melt sequence release classes. Of these, six release classes had individual frequency below the cutoff value used, 5E-10 per year. These six release classes had a total frequency of 6.21E-10 (0.005 % of the total core damage frequency) and were deleted from further consideration. The remaining 38 release classes consisted of 10 early core melt sequence release classes, 14 delayed core melt sequence release classes, and 14 late core melt sequence release classes.

The IPE team defined early containment failure as that occurring either at or within one hour of reactor vessel failure (section 4.5.2.5, p. 4.5-3). The team defined late containment failure as that occurring later than one hour of reactor vessel failure (section 4.5.2.6, p. 4.5-4).

In the containment performance analysis, the IPE team conservatively assumed that any SGTR that resulted in core melt would subsequently have either a cycling or a "stuck" open MSSV; they therefore categorized this type of event as a containment isolation failure. This treatment is also conservative in terms of radiological releases; some of these sequences could result in a basemat melt-through with lower releases since a large fraction of SGTRs were expected to be depressurized and isolated before significant core uncovery.

The submittal notes the following with respect to reporting on the selection of important severe accident sequences (section 4.7.3, page 4.7-43):

> There are no functional sequences that have a core damage frequency greater than or equal to 1.00E-06 per reactor year and lead to a containment failure which can result in a radioactive release magnitude greater than or equal to the PWR-4 release categories of WASH-1400.

The IPE team's characterization of release categories appears to be complete.

2.3 Quantitative Assessment of Accident Progression and Containment Behavior

2.3.1 Severe Accident Progression.

The submittal provides a detailed overview of the severe accident phenomenological issues on the following and their relationship to the various postulated containment failure modes of the FCS Unit 1 PRA (section 4.2, pages 4.2-1 through 4.2-148):

- External vessel cooling
- Mechanisms of early containment failure (direct containment heating (DCH), hydrogen combustion, steam generation, missile generation, cavity overpressure, and corium debris impact on the containment shell liner)
- Mechanisms of late containment failure (gradual containment overpressurization, basemat melt-through, temperature induced penetration seal failure, and delayed combustion)
- Fission product release, transport, and retention

External Vessel Cooling. As shown in figure 1 of this report (reproduced from figure 4.2.1.1, page 4.2-10 of the submittal), the FCS reactor vessel sits partially below the bottom floor of the containment with about 12.5 feet of the reactor vessel residing below the emergency safeguards recirculation pump. Therefore, the vessel is expected to be submerged significantly for all reactor transients that either use containment recirculation (e.g., LOCAs) or provide sufficient containment spray flow to fill the emergency sump. After reviewing the cavity geometry, available water sources, and the results of the plant accident simulations performed with MAAP computer code, the IPE team found that the loss of sufficient inventory to cover the core would result in submergence of the reactor vessel lower head if containment heat removal is maintained.

Early Combustion-Engineering designs were amenable to this vessel cooling because top-mounted instrumentation designs resulted in a penetration-free and instrumentation-free lower head. Thus, submergence of the reactor vessel lower head would be expected to better survive the corium attack-external vessel cooling process. In modeling the external vessel cooling process, the FCS IPE team considered the following in defining success:

- Availability of continuous internal water sources
- RCS pressure
- Water level in the reactor cavity

Note that although the cavity flooding would enable external vessel cooling, it increases the likelihood of occurring ex-vessel steam explosions in the event of vessel failure.

Mechanisms of Early Containment Failure. The IPE team found that the FCS design was expected to substantially mitigate containment threats from high pressure melt ejection (HPME) and direct containment heating (DCH) processes. FCS DCH mitigation features included 1) the availability of a PORV to reduce RCS pressure in the vicinity of, or below, the debris entrainment threshold (not credited in the PRA), and 2) the presence of a concrete floor located about 10 feet above the cavity manway exit to aid in de-entraining and retaining the bulk of the corium debris in the lower containment. In addition to the above features, the FCS cavity is designed to be passively flooded before reactor vessel lower head failure. Ejection of debris into a deep water pool would minimize the containment overpressurization threat from the HPME.

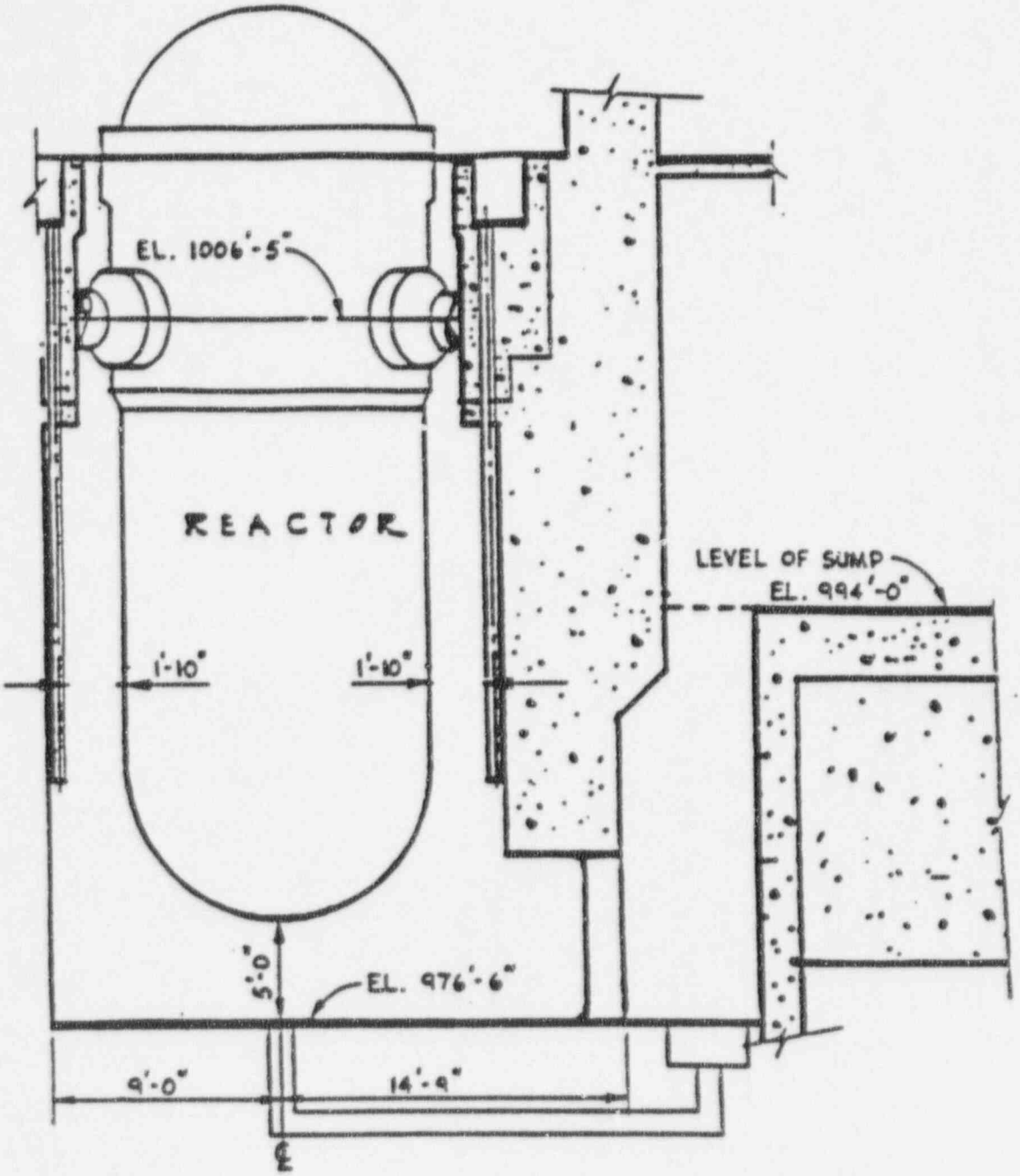


Figure 1. Fort Calhoun Station Unit 1 reactor cavity (reproduced from figure 4.2.1.1, page 4.2-10 of the submittal).

Using a two-cell DCH model as developed by M. Piltch of Sandia National Laboratories, median discharges at vessel breach, and FCS composite fragility curve, the IPE team calculated the following conditional containment failure probabilities for DCH for high pressure discharges: 1) in the presence of a pre-vessel breach hydrogen burn, < 0.08 and 2) without a pre-vessel breach hydrogen burn, < 0.15. For intermediate pressure discharges (RCS pressure < 1200 psia), the conditional containment failure was calculated to be less than 0.005.

The peak containment pressure resulting from rapid steam generations events following an FCS reactor vessel lower head breach were calculated for selected severe accident scenarios as follows:

- Station blackout, < 75 psia (design basis)
- "V" sequence LOCA, < 75 psia (design basis)
- Large LOCA without containment sprays available, ~ 135 psia

The IPE team calculated that rapid steam generation events would not result in a significant challenge to the FCS containment.

The IPE team found that the potential for hydrogen detonation within the FCS containment was remote before vessel breach but possible after vessel breach in "dry" containment environment.

Conditional probabilities that a hydrogen burn would either be initiated as, or become, a detonation were defined as follows (section 4.2.2.3.2.7, page 4.2-62):

- For accident scenarios where the steam concentration was expected to exceed 30 % by volume, detonations were not considered credible. Because of the large steam release associated with the HPME, DCH events were not considered precursors to detonations.

- For hydrogen concentration below 13 % by volume, detonations within the containment were considered impossible. This condition prevailed for pre-vessel breach situations at FCS.

- For conditions where the global hydrogen concentration was expected to be above 13 % by volume and steam concentration was below 30 % by volume (i.e., containment heat removal was successful), the fraction of hydrogen burns that might become detonations was taken to be 0.10 for sequences which discharge hydrogen directly to the containment.

It was assumed that the occurrence of a detonation would fail containment with a probability of 0.50.

Because of the special design feature that encloses all major RCS components within concrete structures, containment failure from direct impingement of debris was considered unlikely.

After comparing the post-vessel breach cavity pressure of 160 psia that was calculated using MAAP with the design strength of 220 psia, the IPE team concluded that cavity integrity would not be threatened.

For scenarios where vessel breach occurred at high RCS pressure, the IPE team calculated that the conditional probability of rocket induced containment failure was 1.75E-3. For medium pressure vessel breach, the rocket failure probability was taken to an order of magnitude lower.

Late Containment Failure. The IPE team considered steam overpressurization failure of the containment before and after vessel breach. The containment could fail before vessel breach when the containment heat removal function is irrecoverably lost (e.g., via loss of CCW) and cooling of the RCS with a breach (either due to pipe rupture or open PORV) is facilitated. Containment failure before vessel breach was calculated to have a frequency of 1E-10 per reactor year and therefore did not show up as a dominant containment failure mode in the PRA.

If active core heat removal systems (containment sprays and/or fan coolers) are unavailable, the steam addition will pressurize the containment to the point of failure. MAAP calculations for FCS showed that the availability of one train of a containment heat removal system (sprays or fan coolers) will be sufficient to control containment pressure well below the ultimate failure pressure threshold.

Overpressurization in the presence of non-condensibles was also evaluated. The maximum amount of non-condensibles to be evolved during the concrete thermal decomposition was found to yield about 1100 lbm-moles of hydrogen and about 2000 lbm-moles of carbon dioxide. These non-condensibles and uncombusted hydrogen produced during oxidation of total core zircaloy inventory and total containment aluminum inventory (from fan coolers) were calculated to raise the containment pressure to 75 psia. Therefore, a concrete attack scenario sufficient to fail the containment via overpressure was not considered credible.

Because of the following FCS features, basemat penetration scenario for FCS was considered to be relatively benign:

- Low core power level (1500 MWt)
- Large reactor cavity floor area
- Passively flooded cavity following a variety of core melt scenarios
- 13-feet thick basemat

Wet cavity sequences comprised greater than 90 % of all core melt scenarios that did not bypass containment. The remaining dry cavity sequences were expected to result in basemat melt-through within several days to a week following the initial corium concrete attack. However, as noted in section 2.2.3 of this report, the dry cavity sequences were found to initiate from SGTRs and were categorized as containment isolation failures in radiological release characterization.

The late hydrogen burn issue was addressed by considering combustion of hydrogen equivalent of 130 % oxidation of the corewide zirconium. Without early burn or DCH occurring 2000 lbm of hydrogen was calculated to burn which was limited by oxygen availability in the containment. The resultant pressure generated was 205 psia which had a probability of containment failure of 0.25.

In addressing phenomenological issues applicable to FCS, the IPE team has extensively used previous work including experiments, and extensive descriptions of phenomena are presented in the submittal.

2.3.2 Dominant Contributors: Consistency with IPE Insights.

Tables 3 and 4 below show SCIENTECH comparisons of the FCS conditional containment failure probability with the results of other IPEs and Zion/NUREG-1150. The CDF for FCS is in the mid range of the values shown in the tables; the FCS containment failure probabilities are in line, except the following, with those of the other plants:

- Several plants have zero probability of early containment failure; IPEs of these plants used phenomenological issue papers to address severe accident issues and found that early containment failure would not be a threat to each of the containments.

- FCS has comparatively higher probability of isolation failure, with the exception of Diablo Canyon. The major reason was that the FCS IPE team categorized SGTR as isolation failure.

2.3.3 Characterization of Containment Performance.

The FCS IPE team used CETs to characterize containment performance under severe accident sequences. The CETs and associated support logic models (SLMs) were quantified using the CAFTA GTPROB module. The six CETs were converted to three master CET fault trees, one for each core melt timing class (early, delayed, and late). The top event on each of these fault trees was defined as "Release Occurs." This event was defined as an OR gate with proper release classes (CET endpoints) as the first level inputs to this event. The logic for each release point element was defined based on the path through the corresponding CET for that release class and the SLMs. These models

Table 3. Conditional Containment Failure Probability During Mission Time (Percent)

Study	CDF per rx yr	Early Failure	Late Failure	Bypass	Isolation Failure	Intact
Diablo Canyon IPE	8.8E-5	4.6	45.2	1.8	7	41.4
Maine Yankee IPE[1]	7.4E-5	8	48	2.1	*	43
Palo Verde IPE	9.0E-5	10	14	4	0[2]	72
Kewaunee IPE	6.6E-5	0	0	8	0.023	92
Zion IPE	4.0E-6	0	5	30	2	63
Haddam Neck IPE	1.8E-4	0.18	54	6.5	0.5	39
Point Beach IPE	1.0E-4	0	0	6.1	0.031	94
Farley IPE	1.3E-4	0	3.1	0.36	0.06	96.4
Zion/NUREG-1150	6.2E-5	1.5	25	0.5	na	73
San Onofre IPE	3.0E-5	0	9.4	6.7	0.07	83.8[3]
Vogtle IPE	4.9E-5	0	0	3.4	0.4	96.2
Callaway IPE	5.8E-5	0.2	52.8	2.0	0	45.0
Fort Calhoun IPE	1.4E-5	1.6	28.0	5.4	5.1[4]	59.8

* Bypass and isolation combined

na Not available

1 Values do not add to "100"

2 Probability is less than 0.001, conditional on core melt

3 Includes MCCI basemat penetration failures

4 Includes SGTR

Table 4. Conditional Containment Failure Probability Beyond Mission Time (Percent)

Study	CDF rx yr	Early Failure	Late Failure	Bypass	Isolation Failure	Intact
Diablo Canyon IPE	8.8E-5	4.6	66.6	1.8	7	20
Maine Yankee IPE[1]	7.4E-5	8	48	2.1	*	43
Palo Verde IPE	9.0E-5	10	14	4	0[2]	72
Kewaunee IPE	6.6E-5	0	49	8	0.023	43
Zion IPE	4.0E-6	0	5	30	2	63
Haddam Neck IPE	1.8E-4	0.18	54	6.5	0.5	39
Point Beach IPE	1.0E-4	0	17.4	6.1	0.031	76.6
Farley IPE	1.3E-4	0	96.2	0.36	0.06	3.3
Zion/NUREG-1150	6.2E-5	1.5	25	0.5	na	73
San Onofre IPE	3.0E-5	0	9.4	6.7	0.07	83.8[3]
Vogtle	4.9E-5	0	76.1	3.4	0.4	20.1
Callaway IPE	5.8E-5	0.2	52.8	2.0	0	45.0
Fort Calhoun IPE	1.4E-5	1.6	28.0	5.4	5.1[4]	59.8

* Bypass and isolation combined

na Not available

1 Values do not add to "100"

2 Probability is less than 0.001, conditional on core melt

3 Includes MCCI basemat penetration failures

4 Includes SGTR

were sequentially solved for all of the PDSs using GTPROB and the PDS dependent basic event probabilities (listed in table 4.6.2 of the submittal).

Overall, the containment remained intact 59.8 % of the time following a severe accident. Consequently the containment failed 40.2 % of the time for these sequences. The percentage of intact containment without accompanied vessel breach occurring was 26.0 %.

Following were the contributions for 40.2 % of the containment failures (alpha mode failure and basemat melt-through failures were negligible):

- Late containment failure 28.0 %
- Bypass (interfacing systems LOCAs - 4.9 % and SGTR - 0.5 %) 5.4 %
- Containment isolation failure 5.1 %
  (isolation valve failure - 0.13 % and SGTR - 5.0 %)
- Early containment failure 1.6 %

Late containment failures at Fort Calhoun are dominated by containment overpressure. Early containment failures at Fort Calhoun are dominated by hydrogen burn, DCH, and ex-vessel steam explosions.

The submittal notes the following on the above results (section 4.7.2.4, pages 4.7-40 and 4.7-41):

- Almost 60 % of the core damage sequences would result in intact containment which was facilitated mainly from the FCS design which 1) provided redundant means of long-term containment heat removal and 2) was sufficiently robust in its plant performance characteristics and containment strength to benefit from power recovery.

- Containment failure sequences were dominated by late containment overpressure failure which are associated with the Level 1 finding that a large fraction of accident scenarios which resulted in core melt also disabled the containment heat removal system. This combination would occur for all unrecovered station blackout scenarios, and core melt scenarios with complete loss of either Raw Water or CCW.

- The low conditional early containment failure probability was a consequence of the high containment pressure capacity and robust reactor cavity. Detailed structural analysis performed on FCS Unit 1 showed that the median failure strength of the FCS containment was greater than 3.5 times the design pressure compared to typical PWR dry containment capacity values of 2.5 to 3 times the design pressure. At the FCS ultimate pressure levels, containment overpressure scenarios caused by either hydrogen burn or DCH posed a small containment threat. Also, steam explosion threats associated with failure of the reactor vessel

lower head in the presence of water also posed a small threat to containment integrity.

- Basemat melt-through could occur during transients with dry reactor cavity conditions which were possible only during the sequences that deposited reactor inventory outside the containment building. This would occur for both ISLOCAs and SGTRs which were categorized as early containment releases; therefore, late containment failure was not considered. By assuming that 50 % (or more) of the SGTRs were successfully isolated just before full inventory depletion, the IPE team calculated that containment isolation failure would reduce to 3.5 % and the basemat melt-through containment failure would increase to 2.2 % of the overall CDF.

2.3.4 Impact on Equipment Behavior.

The submittal notes the following with reference to impact on equipment behavior (section 4.1.2.7, pages 4.1-29 and 4.1-30, reference 1):

> An engineering analysis (EA-FC-9226) was done to determine the ability of instrument and power cable to withstand extreme temperature. The cables are rated from the manufacturer to be able to survive 100 hours at 266 °F. Testing was also done to determine that cables could withstand 700 °F for a short period of time such as would occur with hydrogen burn.

The licensee response to the staff's RAI notes the following pieces of primary equipment/components necessary to mitigate the radiological consequences of a severe accident: 1) containment penetrations (electrical and mechanical), and 2) containment heat removal equipment (containment sprays and containment fan cooler units). FCS penetration seals were found to survive for sequences where containment failure was not otherwise expected.

Operation of either the containment spray system or the fan cooler units was essential to ensure containment integrity following a severe accident. For the containment spray system, the spray valves and pumps were located outside the containment and therefore were not subject to harsh environments.

The fan coolers were recirculation heat exchangers located within the containment. FCS had two containment cooling units and two containment cooling and filtering units.

2.3.5 Uncertainty and Sensitivity Analysis.

The IPE team performed sensitivity studies on the effects of the following on the back-end results (section 4.10):

- RCS depressurization before vessel breach
- External vessel cooling and debris retention within the reactor vessel
- Ex-vessel steam explosions and rapid steam generation
- Containment integrity
- Hydrogen burn prior to vessel breach
- No recovery of offsite power (i.e., no recovery of containment heat removal or containment sprays)

Of these, the effect of no recovery of offsite power was found to have the greatest impact on the back-end results. For this case, the conditional probability (given core melt) that the containment is intact decreased by 33.0 % and the conditional probability of late containment failure increased by 32.8 % from the base case.

For all the other sensitivity studies, changes were not dramatic, even with large variations in basic event values. For example, by increasing the conditional probability of an ex-vessel steam explosion occurring, given vessel breach to a value of 1.0, the conditional probability of early containment failure increased by only 2.2 % and that of late containment failure decreased by only 0.94 % from the base case.

2.4 Reducing Probability of Core Damage or Fission Product Release

2.4.1 Definition of Vulnerability.

The licensee response to the NRC staff's RAI provides the following information (response 32, reference 2). The IPE team retained all the sequences that met the guidelines in NUMARC 91-04. In performing the containment performance analyses, the IPE team coupled all retained core damage sequences with the containment safeguards sequences to generate PASs. They mapped all PASs with a frequency of greater than or equal to 1E-9, or which covered potential vulnerabilities, into PDSs. They mapped all PDSs into release classes by being propagated through the CET. The IPE team used all release classes with frequency greater than 5E-10 in the calculation of risk. The IPE team reviewed the retained release classes for potential containment vulnerabilities. They found no severe accident vulnerabilities unique to the plant.

2.4.2 Plant Improvements.

The plant improvements related to the IPE involved with the front-end analysis (table 6-2 of the submittal).

2.5 Responses to CPI Program Recommendations

As a result of the Containment Performance Improvement (CPI) program, recommendations were made for consideration by licensees as part of the IPE process. These recommendations were identified in Generic Letter 88-20, Supplement 3. The recommendation applicable to the FCS is as follows:

Licensees with dry containments are expected to evaluate containment and equipment vulnerabilities to localized hydrogen combustion and the need for improvements (including accident management procedures) as part of the IPE.

In response to the NRC staff's RAI, the licensee notes the following (response 39, reference 2):

> The containment structure was walked down and prints were reviewed to determine if there were hydrogen "pockets" where hydrogen could cause equipment needed for accident mitigation to be damaged. No vulnerabilities were found, i.e., no pockets were found where damage to equipment would occur.

2.6 IPE Insights, Improvements, and Commitments

Following were the insights gained by performing the FCS IPE:

- No severe accident vulnerabilities associated with FCS had been found.
- The safety injection and containment spray pumps were installed in large rooms rather than compartments. The pumps were therefore capable of operating for an extended period without heating, ventilation, and air conditioning.
- The transfer of safety injection and containment spray systems from the injection mode to the recirculation mode was accomplished entirely from the control room. No human actions outside of the control room were required.
- High pressure safety injection, low pressure safety injection, and containment spray pumps required cooling water only in the recirculation mode. Cooling water was not required in the injection mode.
- The high pressure safety injection pumps took suction directly from the containment sump in the recirculation mode. Intermediate booster pumps were not required.
- FCS was a relatively compact plant. Areas outside the control room in which human actions would be performed could be reached quickly and easily. This increased the probability that an action would be successfully performed within the allowable time period.
- Raw water served as a manually-aligned backup to component cooling water for the shutdown cooling heat exchangers, containment cooling units, safety injection and containment spray pump bearing coolers, and control room air conditioners.

- FCS used air-operated valves for many applications compared to the generally used motor-operated valves. Generic data showed that the failure probability for air-operated valves was lower than that for motor-operated valves. In addition, the air-operated valves normally failed to their accident positions, reducing the vulnerability to station blackout. For example, normally open containment isolation valves typically failed closed upon loss of air or loss of power.

- The FCS large dry containment design provided adequate capability to mitigate severe accidents. No unusually poor containment performance had been found.

- Flooding of the reactor cavity allowed for retention of corium within the reactor cavity for about 26 % of PDSs. Successful cavity flooding reduced short term containment failure due to HPME and reduced radiological releases from the reactor coolant system. This lessened the impact of DCH.

- For situations where the reactor vessel lower head failed, the ability to flood the reactor cavity provided for ex-vessel cooling of corium on the cavity basemat. The large FCS basemat and low core power resulted in a high likelihood that overlying water would cool the corium debris.

- As a result of the high strength of the FCS containment, the conditional probability of early containment failure (given core melt) was relatively low (1.62 %). The most significant early containment threats were associated with hydrogen burns following vessel breach and steam explosions in the reactor cavity.

- A key feature of the FCS containment design was that for about 75 % of the accident sequences, the reactor cavity was flooded with water. This decreased the likelihood of reactor vessel failure (due to ex-vessel cooling) and resulted in lower releases (due to retention of fission products by the water) compared to vessel failure with the core falling on a dry cavity floor.

- A diesel-driven fire pump, independent of plant support systems, was available for long-term makeup to the emergency feedwater storage tank. This pump could also serve as a backup to the raw water system for the purpose of cooling the component cooling water system.

- The architectural design of the reactor cavity and the drains in containment lead to ex-vessel cooling of the reactor vessel for all no-interfacing LOCAs and prevented or delayed vessel breach.

- The containment ultimate pressure analysis determined that the failure pressure was more than three times the design pressure.

- The pathways from the reactor to the rest of containment is tortuous, and corium could not have contact with penetrations that could breach containment integrity.

- In containment, both the fans and the sprays had the ability to cool the containment atmosphere independently. This redundant cooling was important for containment integrity and equipment operability.

- The thickness of the basemat of 13 feet was in excess of what was required to prevent the core from melting through the containment.

- FCS was equipped with a hardened vent for potential use in hydrogen purge activities, This venting was not proceduralized; however, during a severe accident, the hydrogen vent could be used as a mechanism to guarantee containment integrity and establish a controlled release.

3. CONTRACTOR OBSERVATIONS AND CONCLUSIONS

The IPE submittal notes the following on back-end results:

- Almost 60 % of the core damage sequences would result in intact containment which was facilitated mainly from the FCS design which 1) provided redundant means of long-term containment heat removal and 2) was sufficiently robust in its plant performance characteristics and containment strength to benefit from power recovery.

- Containment failure sequences were dominated by late containment overpressure failure which are associated with the Level 1 finding that a large fraction of accident scenarios which resulted in core melt also disabled the containment heat removal system. This combination would occur for all unrecovered station blackout scenarios, and core melt scenarios with complete loss of either Raw Water or CCW.

- The low conditional early containment failure probability was a consequence of the high containment pressure capacity and robust reactor cavity. Detailed structural analysis performed on FCS Unit 1 showed that the median failure strength of the FCS containment was greater than 3.5 times the design pressure compared to typical PWR dry containment capacity values of 2.5 to 3 times the design pressure. At the FCS ultimate pressure levels, containment overpressure scenarios caused by either hydrogen burn or DCH posed a small containment threat. Also, steam explosion threats associated with failure of the reactor vessel lower head in the presence of water also posed a small threat to containment integrity.

- Basemat melt-through could occur during transients with dry reactor cavity conditions which were possible only during the sequences that deposited reactor inventory outside the containment building. This would occur for both ISLOCAs and SGTRs which were categorized as early containment releases; and therefore, late containment failure was not considered. By assuming that 50 % (or more) of the SGTRs were successfully isolated just before full inventory depletion, the IPE team calculated that containment isolation failure would reduce to 3.5 % and the basemat melt-through containment failure would increase to 2.2 % of the overall CDF.

The FCS IPE submittal contains a substantial amount of information with regard to the recommendations of GL 88-20, its supplements, and NUREG-1335. The submittal appears to be complete in accordance with the level of detail requested in NUREG-1335. The methodology used to perform the IPE is described clearly in the submittal. The approach taken, which is consistent with the basic tenets of GL 88-20, Appendix 1, is also described clearly along with the team's basic underlying assumptions. The important

plant information and data are well documented and the key IPE results and findings are well presented.

The IPE team found no severe accident vulnerabilities unique to the FCS. They identified no back-end plant improvements.

4. REFERENCES

1. Omaha Public Power District "Fort Calhoun Station IPE, Final Report," December 1993.

2. Omaha Public Power District "Response to Request for Additional Information on Fort Calhoun Station IPE Submittal," November 1995.

3. Oracle Corp., "SQL*FORMS Designers Reference," 1986.

4. Swanson Analysis Systems, Inc., Houston, PA, "ANSYS-PC/LINEAR Reference Manual," 1987.

Appendix
IPE Evaluation and Data Summary Sheet

PWR Back-End Facts

Plant Name

Fort Calhoun Unit 1

Containment Type

Large, dry

Unique Containment Features

- A diesel-driven fire pump, independent of plant support systems, was available for long-term makeup to the emergency feedwater storage tank. This pump could also serve as a backup to the raw water system for the purpose of cooling the component cooling water system.

- The architectural design of the reactor cavity and the drains in containment lead to ex-vessel cooling of the reactor vessel for all non-interfacing LOCAs and prevented or delayed vessel breach.

- The pathways from the reactor to the rest of containment is tortuous, and corium could not have contact with penetrations that could breach containment integrity.

- In containment, both the fans and the sprays had the ability to cool the containment atmosphere independently. This redundant cooling was important for containment integrity and equipment operability.

- The thickness of the basemat of 13 feet was in excess of what was required to prevent the core from melting through the containment.

- FCS was equipped with a hardened vent for potential use in hydrogen purge activities. This venting was not proceduralized; however, during a severe accident the hydrogen vent could be used as a mechanism to guarantee containment integrity and establish a controlled release.

Unique Vessel Features

Similar to other early Combustion-Engineering designs, FCS reactor vessel was amenable to external cooling because top-mounted instrumentation designs resulted in a penetration-free and instrumentation-free lower head. Thus, submergence of the reactor vessel lower head would be expected to better survive the corium attack-external vessel cooling process.

Number of Plant Damage States

45

Ultimate Containment Failure Pressure

215 psig (median or 50th percentile value)

Additional Radionuclide Transport and Retention Structures

Release mitigation by auxiliary building is credited

Conditional Probability that the Containment Is Not Isolated

0.00056 (mainly from SGTRs)

Important Insights, Including Unique Safety Features

- Flooding of the reactor cavity allowed for retention of corium within the reactor cavity for about 25 % of PDSs. Successful cavity flooding reduced short-term containment failure due to HPME and reduced radiological releases from the reactor coolant system. This lessened the impact of DCH.

- For situations where the reactor vessel lower head failed, the ability to flood the reactor cavity provided for ex-vessel cooling of corium on the cavity basemat. The large FCS basemat and low core power resulted in a high likelihood that overlying water would cool the corium debris.

- As a result of the high strength of the FCS containment, the conditional probability of early containment failure (given core melt) was relatively low (1.62 %). The most significant early containment threats were associated with hydrogen burns following vessel breach and steam explosions in the reactor cavity.

- For about 75 % of the accident sequences, the reactor cavity was flooded with water. This decreased the likelihood of reactor vessel failure (due to ex-vessel cooling) and resulted in lower releases (due to retention of fission products by the water) compared to vessel failure with the core falling on a dry cavity floor.

Implemented Plant Improvements

No back-end plant improvements are considered

C-Matrix

C-Matrix can be generated from the information provided in table 4.8.2-4, pages 4.8-19 through 4.8-22 of the submittal.

DRAFT

STANDARD REVIEW PLAN

USE OF PRA IN REGULATORY ACTIVITIES

TABLE OF CONTENTS

DRAFT

STANDARD REVIEW PLAN

USE OF PRA IN REGULATORY ACTIVITIES

19.0 GENERAL GUIDANCE

INTRODUCTION

The purposes of this standard review plan (SRP) are to identify the roles and responsibilities of organizations in the NRC that participate in risk-informed reviews of regulated activities and provide general guidance to the NRC staff for evaluating information from a plant specific probabilistic risk assessment (PRA) submitted for staff review. The SRP identifies the types of information, that may be used in each activity and provides general guidance on how the information from the PRA can be combined with other pertinent information in the process of making a regulatory decision.

The guidance in this document is a logical extension of current NRC policy on the use of PRA in regulatory activities which is documented in the staff's PRA policy statement and PRA implementation plan (references 1, 2 and 3). In developing this document, the staff has considered the relevant industry guidance documented in Reference 4 and the NRC regulatory guide on the use of PRA in risk-informed regulatory applications, Regulatory Guide DG-1061 (Reference 5). Throughout this document, reference will be made to other SRP chapters which provide detailed guidance for the review of specific applications of PRA in regulated activities.

Risk-informed decision making will be based on the following approach. The PRA analyses should be unbiased (i.e., not deliberately conservative), and should address significant uncertainties. Results of these risk analyses will be one of several inputs to the decision process that evaluates margin in plant capability (both in physical performance and in redundancy/diversity). The decision process should supplement risk results with consideration of defense in depth as a means of addressing issues of incompleteness in risk modeling. Risk analysis will inform, but will not determine regulatory decisions.

ROLES AND RESPONSIBILITIES

Depending on the technical nature of a licensee's request, an appropriate technical review branch in NRR will serve as the primary review branch; and as such, has overall responsibility for leading the technical review, drafting the staff safety evaluation report (SER) or other regulatory document, and coordinating inputs from other technical review organizations. The responsibilities of specific review organizations that will normally play a role in reviewing risk-informed proposals are listed below.

The Probabilistic Safety Assessment Branch (SPSB) has primary responsibility for review of the PRA information submitted by the licensee including: the overall scope, level of detail and quality of the PRA; the accuracy and completeness and of all level 1 PRA (front end) information; the adequacy and appropriateness of the PRA for each particular application; and the selection and application of numerical decision criteria. Support for the review in the area of system modeling is provided, as needed, by the technical review branch in NRR that is responsible for the review of information regarding the system. Support in reviewing the selection of PRA scope and level of detail is provided by the lead NRR technical branch for the PRA application (e.g., the Mechanical Engineering Branch for Inservice Testing).

The Reactor Systems Branch (SRXB) provides support to SPSB as necessary in the area of accident sequence modeling, including treatment of reactivity and thermal-hydraulic phenomena (e.g., criteria for avoiding core melt), the implementation of emergency operating procedures and abnormal operating procedures and system response, and issues regarding operations when the plant is in a shutdown condition.

The Containment and Severe Accident Branch (SCSB) has primary responsibility for review of the accuracy and completeness of all level 2 PRA information submitted by a licensee in support of a request for regulatory action.

The Emergency Preparedness and Radiation Protection Branch (PERB) has primary responsibility for review of the accuracy and completeness all level 3 PRA information submitted by a licensee in support of a request for regulatory action.

The Office of Research (RES) At the request of NRR, RES provides technical support to primary review branches in NRR in areas involving all levels of PRA.

The Office for Analysis and Evaluation of Operational Data (AEOD) conducts system reliability studies and compiles generic and plant specific data on the frequency of initiating events, common cause failures and human errors from operating experience. This information is available to reviewers and can be used for independent verification of data used in PRAs submitted by licensees and applicants. In addition, AEOD conducts the Accident Sequence Precursor Program which is used to screen operating reactor events for safety significance. Information from this program should be used when reviewing applications which involve PRA assessments of reactor events, e.g., enforcement issues.

I. AREAS OF REVIEW

The NRC's PRA Implementation Program plan (reference 1) identifies a wide scope of regulatory activities for which PRA can play a role. This scope includes activities which require NRC review and approval and other activities which are considered internal to NRC and affect licensees and applicants in a less direct manner, e.g. generic issue prioritization. This Standard Review Plan chapter deals only with those activities submitted for NRC review and approval for which the staff has concluded PRA can play a role in the decision-making process. General review guidance for applicable activities is presented in this SRP. In addition, application-specific SRP chapters are available to provide more detailed guidance for several activities. Currently, these include:

Changes to allowed outage times (AOT) and surveillance test intervals (STI) in plant specific technical specifications;

Changes in scope and frequency of tests on components in a licensee's inservice test (IST) program;

Changes in scope and frequency of inspections in a licensee's inservice inspection (ISI) program;

Grading of activities in the licensee's quality assurance (QA) program.

In addition to the above, other activities which could involve a risk-informed decision making process include:

Safety evaluations regarding plant specific design issues and plant specific backfit evaluations;

Justification for continued operation proposed by licensees in light of non-conforming conditions;

Technical bases supporting notices of enforcement discretion;

Review of a design-specific PRA submitted per section 10 CFR 52.47 of the regulations;

Integrated assessment of groups of plant modifications which taken together result in a net decrease or no net increase in risk.

Review guidance provided in this SRP applies to all risk-informed application submittals and supplements application-specific SRPs where these exist. All provisions in this SRP apply to all applications except where an application-specific SRP specifically indicates otherwise.

The scope of the staff review of a risk-informed application will be specific to the application itself. However, this scope should include the review of a six-element approach as suggested in the general Reg Guide for risk-informed decision making (Reg Guide DG-1061, reference 1). The areas of review for each of these elements are discussed below. Alternatives to this six-element process may be acceptable if the reviewer can determine that an equivalent approach (i.e., addressing both deterministic and probabilistic risk issues) has been submitted.

Element 1 - Characterization of the proposed regulatory change

For this element, the reviewer should look at the nature of the proposed change and how this change is to be modeled in the PRA. To accomplish this, the reviewer has to identify the elements of the PRA on which the proposed change is expected to have an impact, and to develop appropriate methods of mapping the impact of the change onto those PRA model elements. This would lead to a definition of the deterministic and probabilistic engineering evaluations needed to support the change. The reviewer should verify that licensee evaluation methods were supportable by available information, and that the plant PRA and the deterministic analyses are capable of reflecting the impact of the changes.

Element 2 - Conduct of a deterministic engineering evaluation of the proposed change

The reviewer should ensure that the proposed changes do not unduly compromise the intent of the existing licensing basis (NRC requirements, licensee commitments, and plant specific design basis). Therefore, the scope of the review in this element should

include consideration of the current design basis and compliance requirements (including industry codes and standards, when relevant) and general design criteria. In addition, the maintenance of the defense in depth philosophy, balance between prevention and mitigation, pertinent engineering data and analysis, plant operating experience, and potential compensatory measures are essential elements of the staff review and should be evaluated in terms of how they would be used to supplement risk insights from a PRA.

Element 3 - Evaluation of the nature of the contribution of the proposed change to plant risk

In this element the review should focus on the evaluation of the effects of the proposed changes on equipment functionality, reliability and availability and on the impact of these changes on plant risk. Considerations should be given to the correct application of the PRA in these areas.

As part of the review, the requirements of the PRA for each application in terms of scope, level of detail, and PRA quality have to be addressed. In the area of PRA quality, attention has to be paid to technical issues like the modeling of success criteria, common cause failures, and human reliability. Potential limitations of the PRA model in terms of truncation limits, screening criteria used, analysis assumptions, modeling of initiating events, and modeling of dynamic versus static plant configurations also have to be taken into account. The review of the PRA should be a focussed application-directed review on the specific contributors affected by the proposed changes.

Specifically, the review should assess whether the PRA model is adequate in its coverage of the impact of the change, that is, whether all impacts of the change are reflected in the model, or whether the degree to which the change can be reflected is limited by PRA scope or completeness issues. Recognizing any limitations imposed by the scope or completeness of the PRA, or recognizing any portions of the PRA that, by themselves, will model the proposed change relative to plant risk, will establish an appropriate scope of review and acceptance criteria. This will also effectively identify whether the licensee scope of analysis is appropriate, e.g., whether it is adequate to perform a relatively simple screening analysis; or a ranking analysis where SSCs or other plant elements are ranked relative to one another; or whether absolute or relative changes of risk measures are to be evaluated in a detailed fashion.

Finally, staff activities in this element should include a review of the modification of the PRA models to reflect the cause-effect relationships of the proposed change, and a review of the analyses required for comparison with the acceptance criteria. Assessment of the robustness of analysis conclusions by the performance of appropriate sensitivity and uncertainty analyses should also be carried out as part of the licensee submittal.

In applications where component categorization plays a role in the determination of acceptability of risk, i.e., in cases where SSCs are selected for relaxed regulation as a group based on low risk contributions of the individual SSCs, the process used for component categorization should be reviewed as part of this element.

Element 4 - Development of proposed implementation and performance monitoring strategies

Given that there may not be much available data on the reliability and availability of SSCs under the proposed change to design or operation, careful consideration should be given to the proposed plan for implementation of the change and to performance monitoring strategies for SSCs effected by the change. The review should ensure that the processes will provide early indication of false assumptions and provide criteria for taking actions based on results of monitoring efforts. As such, the review scope should be to ensure that the licensee proposed process for implementation and monitoring is adequate to account for uncertainties with regard to SSC performance under the proposed change.

Element 5 - Determination of the acceptability of the impact from the proposed change

As part of this element, the scope of the review will include an evaluation of the process used to integrate probabilistic insights with deterministic considerations to arrive at a final determination of acceptability. The review of probabilistic results should include an assessment of: the change in risk from the application; the cumulative and synergistic effects from the current and

all previous applications; the potential for creating new vulnerabilities or exacerbate pre-existing vulnerabilities in risk; and the potential for the erosion of multiple success paths.

The review of deterministic results should include an assessment of: the proposed change in light of existing regulations that is part of the licensing basis; available and applicable deterministic engineering results; the consistency of current plant practices and operational data with that modeled in the risk analysis; and the implementation and monitoring strategies.

Finally, the review of the integration process should also include an evaluation of: the proper modeling of cause-effect relationships; the methods used for compensating potential PRA limitations; the treatment of components not explicitly modeled in the PRA; and the use of partial scope PRAs.

Element 6 - Documentation of the analysis and submittal of the request

The review should determine if the submittal documentation is adequate for the staff to evaluate the acceptability of the proposed change. The availability of supporting documentation that is not part of the submittal should also be a review consideration.

II. ACCEPTANCE CRITERIA

Guidance criteria for the reviews of applications in risk-informed regulation (RIR) are provided in the sub-sections below. Sub-section II.1 documents general guidance criteria. Sub-section II.2 documents the requirements needed for the characterization of a proposed regulatory change. Sub-sections II.3 and II.4 provide general criteria for deterministic and probabilistic evaluations respectively. A quality PRA (scope, level of detail, truncation, etc.) is central to all risk-informed efforts, and the general acceptance criteria for determining the quality of PRAs are included in sub-section II.4. Criteria for the proper implementation of the proposed change and criteria for monitoring of performance of equipment covered by the change are provided in sub-section II.5. Finally, general criteria for the integration of probabilistic and deterministic considerations (including the use of expert panels) are provided in sub-section II.6. The results from the integration will form the basis for potential risk-informed regulatory changes.

II.1 General Guidance

To effectively review risk-informed regulation approaches, the staff must ensure that the plant's current licensing basis and actual operating condition and practices are properly reflected in the risk estimates using the plant PRA model. Otherwise, the risk assessment may provide inaccurate or misleading information that will require careful scrutinity before use in any regulatory decision-making process.

In order for the staff to make findings of acceptability regarding changes in regulatory requirements or positions, or previous licensee commitments, licensees must present bases which are built from a blend of deterministic and probabilistic information. Specific types of deterministic and probabilistic information which should be included in submittals are described in section 4 of Reg Guide DG-1061. Some general guidelines and criteria for developing an integrated basis for a finding of acceptability are given below:

Assessment of risk importance should reflect not only results from PRAs but also deterministic evaluations such as test results, engineering analysis and operating experience reviews;

When risk insights from a PRA are used to quantify conservatism in original licensing basis analysis, the deterministic requirements that are affected (i.e., being departed from) have to be characterized and re-analyzed to determine whether the original intent of the requirement is still being satisfied;

PRA results and conclusions have to be shown to be robust in terms of the analysis assumptions and uncertainties. Showing robustness does not necessarily mean carrying out uncertainty analyses but can entail sensitivity analyses, bounding analyses, and engineering justifications;

When lack of completeness or uncertainties in the PRA models can affect risk-informed decision making, applicable deterministic information or compensatory actions which can be shown to clearly reduce risk shall be used to assure a conservative outcome;

Net changes in risk from risk-informed applications should optimally reflect improvements in safety or be risk neutral. Any proposed risk increase shall not exceed the criteria specified in Appendix B of Reg Guide DG-1061;

Probabilistic and deterministic methods used to demonstrate the acceptability of proposed changes in requirements for certain SSCs should also be applied to identify changes where tightened controls and oversight on other SSCs would improve safety, i.e., requirements and resources should be re-directed from low risk importance contributors to high risk importance contributors thereby achieving more balanced risk contributions.

The acceptability criteria and requirements for probabilistic and deterministic evaluations in supporting regulatory decision depends in part on the role each of these types of evaluations plays in the determination of the final result. The rigor required of the evaluation should be commensurate with the emphasis placed on the use of the results to support the decision making process. In general, the results from PRA models will not be accepted as the sole basis for changes in regulatory practice. Rather, the results from such models must be supplemented with arguments based on other traditional sources of guidance, including consideration of defense in depth and codified engineering standards.

Finally, reviewers should consider whether or not a relief request is in any way contrary to an applicable code or standard. Generic

requests which go against existing codes or standards should not be accepted for review unless specific regulatory guidance for such applications, i.e., a regulatory guide and standard review plan has been developed.

II.2 Criteria for the Characterization of Change (Element 1)

For a proposed regulatory change to be risk informed, the licensee has to be able to define the change in terms which are compatible with a PRA, i.e., the PRA has to be able to effectively evaluate or realistically bound the effects of the change.

The characterization of the problem has to include the establishment of a cause-effect relationship to identify portions of the PRA affected by the issue being evaluated. This includes (i) identification of the specific PRA contributors for the particular application, (ii) an assessment of the portions of the model which should be modified for the application, and (iii) identification of supplemental tools and methods which could be used to support the application. This will establish criteria for the scope and level of detail of analysis required for the remaining steps of the change process.

II.3 Criteria for Deterministic Evaluations (Element 2)

General criteria for deterministic evaluations are provided in Appendix A of Regulatory Guide DG-1061. In addition, the application specific regulatory guides provide more specific evaluations which are pertinent to each of the applications in question.

In general, proposed changes have to be reviewed with regard to the current design basis, and it has to be shown that a change will not adversely affect the intent of the design basis. Engineering (or other pertinent) analysis and data have to be presented to identify the safety margins or plant activities conducted to preserve those margins. If exemptions from regulations, technical specification amendments, or relief requests are required to implement the licensee's proposed risk-informed program, the appropriate requests should accompany the licensee's submittal.

In addition, results from appropriate deterministic engineering evaluations have to demonstrate that the proposed changes will not compromise sound regulatory and engineering principles such as defense in depth, or compromise the balance between prevention and mitigation. Changes that are found to compromise such principles or balance should either be eliminated from the scope of the proposed change or be packaged with appropriate compensatory measures to maintain the defense in depth philosophy and the balance between prevention and mitigation. Deterministic information sources should include a combination of engineering analyses, plant and industry operational experience, plant-specific performance history, and sound engineering judgement.

II.4 Criteria for Probabilistic Evaluations (Element 3)

In this element a probabilistic risk assessment is performed to evaluate the impact of the proposed changes on quantitative measures of plant risk. Since the scope of these changes could include modifications to plant SSCs, or modifications to testing, maintenance or other operational procedures, the direct impact of the changes will be modeled in equipment functionality, reliability and availability, and in human error probabilities.

The development of a plant specific risk-informed program will require that information be available to identify the application-specific SSCs (and/or human actions) that contribute most significantly to the plant's estimated risk. Components covered shall include:

SSCs whose failure could result in a plant trip.

Safety-related components that are relied upon to remain functional during and following design basis events or severe accidents to ensure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, and the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposure comparable to or in excess of 10 CFR 100 guidelines.

Non-safety-related structures, systems, or components that are relied upon to mitigate accidents or transients or are used in plant emergency operating procedures; or whose failure could prevent safety-related structures, systems, or components from

fulfilling their safety-related function; or whose failure could cause a reactor scram or actuation of a safety-related system.

Human actions covered should include:

those that could directly result in an initiating event;

all pre-initiator events that could result in the unavailability of systems or components (e.g., restoration errors in returning systems or components to their normal state after the completion of maintenance or testing, and miscalibration errors of critical instrumentation); and

response and recovery post-initiator human events. Response actions include those human actions performed in direct response to the accident (i.e., actions delineated by the EOPs). Recovery actions include those human actions performed in recovering a failed or unavailable system or component using available procedural guidance and plant training.

For each basic event directly affected by the proposed application, it is necessary for the licensee process to quantify the event using models that capture all the functional relationships between the application and the basic event. The effect of proposed changes on parameters like common cause failure probabilities and operator errors of commission must also be addressed within the licensee process. In summary, in order for the PRA to support correct decision making, there must be good functional mapping between the application-specific space and PRA model elements.

The results of the determination of the cause-effect relationships between the proposed application and the PRA models will determine the scope and the level of detail required of the PRA to support the application. Sub sections II.4.1 and II.4.2 discuss these criteria. In addition, since the quantitative results of the PRA are to play a major and direct role in the decision making process, it has to be shown that the results are derived from "quality" analyses. The criteria to help determine quality are discussed in sub section II.4.3 and also in Appendix A of this SRP. The criteria for the analysis of PRA model uncertainties relative to determination of risk impacts is provided sub section II.4.4. Finally, the issues related to the determination of risk contribution/component categorization are discussed in Appendix C of this SRP.

II.4.1 Required Scope of Analysis

The required scope of a PRA will depend on the specific application for which the PRA is intended. It is not required for risk-informed regulation that licensees submit Level III PRAs that treat all plant operational modes and all initiators. Instead, when full-scope PRAs are not available, licensees are required to show that the needed findings are supportable based on deterministic, engineering, or other plant operational information that address modes and initiators not analyzed in the base PRA.

For each plant mode not analyzed in the PRA, and for each probabilistically significant initiator in that mode, the licensee has to evaluate the plant capabilities to respond to that initiator. These capabilities can be described in terms of systems, system trains, human actions, etc. that provide some level of redundancy and diversity. The licensee must then show that the proposed change does not unacceptably degrade that capability, that is, that redundancy and diversity still exist in the plant response capability, and that risk vulnerabilities are not introduced by the changes.

This issue is addressed acceptably if:

The licensee addresses all modes and all initiator types using PRA.

OR

The licensee demonstrates that the application does not unacceptably degrade plant capability and does not introduce risk vulnerabilities for any unanalyzed plant modes and initiator types.

OR

If the application potentially impacts unanalyzed plant modes and initiator types, the licensee:

a) advances a suitably redundant and diverse plant response capability for all significant initiators in each mode (see the defense in depth criteria, sub section II.6.2, for redundancy and diversity attributes appropriate for particular initiating events); and

b) ensures that all elements of the plant response capability are within the scope of programmatic activities (IST, GQA, ISI, maintenance, monitoring, etc.) aimed at ensuring satisfactory safety performance; and

c) provides arguments that proposed changes do not introduce vulnerabilities or remove elements of this capability from programmatic activities aimed at ensuring satisfactory safety performance; and

d) provides a bounding analysis on the change in plant risk from the application (e.g., by use of sensitivity studies or use of partition factors as described in Reg Guide DG-1061)

II.4.2 Required Level of Detail

Generally, the PRA has to be detailed enough to account for all important system and operator dependencies (functional, operational, and procedural dependencies). SSCs that are being depended upon for more than one function should be modeled explicitly so that potential dependencies will not be obscured in the evaluation process. Initiating events caused by the loss of support systems should be modeled in detail since the failure of the SSCs that could lead to the initiating events could also result in failure of functions that mitigate that event.

The usefulness of PRA results in risk-informed regulation is dependent on the level of resolution of the modeled SSCs. A component level of resolution provides insights at the component level. However, if a PRA is performed at a system or train level, the insights of the PRA will be limited to the system or train level unless it can be demonstrated that component level insights can be bounded by system or train level effects. The direct application of PRA results will be limited to those SSCs that are explicitly modeled as part of PRA basic events. Insights for SSCs that are implicitly modeled (i.e., screened out, assumed not important, etc.) shall only be used after additional consideration (for example, by an Expert Panel) of the effects of the proposed change on all PRA assumptions, screening analyses and boundary conditions.

II.4.3 Acceptance Criteria for Quality for a PRA for Use in Risk-Informed Regulation

The baseline risk profile is used to model the plant's licensing basis and operating practices that are important to safe operation, and, by implication, areas in which existing requirements can be relaxed without unacceptable safety consequences. Thus, this baseline risk profile provides an indication on how much relaxation may be appropriate. It is therefore essential that the PRA adequately represent the risk profile. To complement this, it is necessary not only to identify significant risk contributors, but also to identify those elements of the plant whose performance is responsible for reducing the risk to acceptable levels, and address these elements adequately in licensee programmatic activities.

Therefore, for risk-informed regulation, the following criteria have to be satisfied.

Reasonable assurance of PRA adequacy: Requirements on PRA adequacy are justified by the important role played by the PRA in supporting the decision process. Criteria for the different quality issues for the licensee's baseline PRA is provided in NUREG-1602 and also in Appendix A of this SRP.

Robustness of results and conclusions: PRA results and conclusions must be robust, and an analysis of uncertainties and sensitivities have to be carried out to show this "robustness". Sub-section II.4.4 discusses criteria for this in more detail.

Key performance elements are appropriately classified and performance is backed up by licensee commitments: PRA results are dependent on plant activities. They reflect not only inherent device characteristics but also numerous programmatic activities, such as IST, ISI, GQA, and so on. Use of a PRA to justify relaxation of a requirement must therefore imply a commitment to whatever programmatic activities are needed to maintain performance at the PRA-credited levels that served as the basis for the proposed relaxation.

II.4.4 Criteria for the Analysis of Model Uncertainties

The uncertainties in the PRA results must be taken into account in the assessment of the risk impact and in the risk-informed decision making process. However, if the risk change due to a proposed application can be verified to be conservative (i.e., a net risk reduction), no uncertainty estimates in the risk change are required.

If the risk change is an increase and is characterized as best estimate, and if the magnitude of the increase is significant (10 percent or greater) compared to the allowable change, then an appropriate consideration of uncertainties must be included to demonstrate the robustness of the results. This uncertainty analysis should include consideration of uncertainty distributions for parameters and models which are used to quantify the application in question. If performed, the analysis of uncertainties should have the following attributes:

It should reflect the data uncertainties associated with each parameter. A Monte Carlo or Latin Hypercube model, or equivalent, is acceptable to estimate the overall uncertainties from the distributions assigned to the individual parameters.

It should account for model uncertainties. There may be several alternate approaches to the analysis of certain elements of the PRA model. The licensee must document that the model that is used is acceptable as defined by NUREG-1602. In certain cases, it may be necessary to perform sensitivity analyses using alternate models to demonstrate the robustness of the conclusions.

It should attempt to address uncertainty that is caused by potential incompleteness of the overall PRA model. The licensee must address the lack of completeness either by demonstrating that the impact of the application on the risk from the missing parts of the PRA is bounded so that the overall impact is acceptable, or by limiting the scope of the application to the SSCs for which the impact on risk can be evaluated.

If the increase in risk from a proposed application is small (10% or less) compared to the allowable change, then an acceptable alternative to explicit uncertainty propagation is to show that events contributing to the change in risk are not associated with significant uncertainty. In order to argue this, the licensee must identify the application-specific events and the compensating events (i.e., events that occur in minimal cutsets along with these application-specific events), and argue that none of these events is associated with significant uncertainty (or by performing sensitivity analyses to show robustness of results). For this purpose, a significant uncertainty is a phenomenological uncertainty, i.e., a large uncertainty associated with an extremely rare event, or an uncertainty associated with a conjunction of events whose rates are causally linked (such as identical check valves in series); in the latter case, cutset uncertainties tend to be significant because the uncertain parameters do not vary independently. The acceptable criterion in this case is that the uncertainty in the change is small compared to the margin between the change and the allowable change.

II.5 Criteria for the Implementation and Monitoring Processes (Element 4)

Decisions concerning implementation of changes should be made in light of the certainty associated with the results of the deterministic and probabilistic engineering evaluations. Broad implementation within a limited time period may be justified when uncertainty is shown to be low (data and models are adequate, deterministic evaluations are verified and validated, etc.), whereas a slower phased approach to implementation would be expected when uncertainty in evaluation findings is higher.

The licensee proposed monitoring program should establish a means to adequately track the performance of equipment covered by the proposed licensing changes. The monitoring plan should be capable of adequately tracking equipment performance after a change has been implemented to demonstrate that performance is consistent with that predicted by the deterministic and probabilistic analyses that were conducted to justify the change. The monitoring plan should assure that any performance degradation is detected and corrected before equipment functionality and plant safety can be compromised. When needed, the program should also include monitoring of similar component performances at other plants to establish a sufficient data base of temporal related degradation. It must be clearly established that sufficient data will be obtained as part of the program to provide statistically significant data, and that the procedures and evaluation methods are implemented which provide reasonable assurance that degradation will be detected.

II.6 Criteria for Integrated Decision Making (Element 5)

The acceptability of a proposed change should include considerations of probabilistic and deterministic criteria. In general, the acceptance of risk-informed changes in regulatory requirements will depend on six elements:

Risk significance of the change;
Maintenance of defense in depth;
Assurance that the change will not create instances of risk imbalance or disproportionate importance of individual items;
Consideration of cumulative and synergistic effects of all changes;
Consideration of deterministic factors; and
Implementation of a performance-based feedback loop.

Criteria for risk acceptance, defense in depth, risk balance, and cumulative effects of risk are provided in sub sections II.6.1 through II.6.4 respectively. Criteria for deterministic evaluations and implementation of a performance based feedback loop are discussed earlier in sections II.3 and II.5 respectively. Finally, sub section II.6.5 provides the criteria for an acceptable process to integrate the above elements for risk-informed applications.

II.6.1 Criteria for Acceptable Risk Impact from Proposed Applications

A quantitative estimate of the total impact of a proposed action, either temporary or permanent, is required for any risk-informed application. This includes the evaluation of the absolute and/or relative changes in risk measures such as core damage frequency (CDF) and large early release frequency (LERF). The necessary sophistication of this evaluation depends on the justification arguments and the magnitude of the potential risk impact. For those actions justified primarily by deterministic considerations and for which minimal risk impact is anticipated, a bounding estimate may be sufficient. For actions justified primarily by PRA considerations for which a substantial impact is possible or is to be offset with compensatory measures, an in-depth and comprehensive PRA analysis is needed.

The numerical risk acceptance criteria for temporary and permanent changes to the plant's risk profile are discussed in Appendix B of Reg Guide DG-1061. In the detailed evaluation of risk significance, the following have to be considered: relative change in risk; change in the baseline risk; risk in terms of CDF, LERF, and frequency of late containment failure. It is necessary to address both internal and external events and all plant operational modes, but it may be possible to accomplish this without a full-scoped PRA in all cases.

II.6.2 Criteria for Assuring Defense in Depth

Proposed plant changes have to maintain defense in depth and have to ensure that multiple lines of defense exist for core damage and large early release mitigation, shutdown risk management, and risk from external events. Therefore, controls should not be completely removed without exhaustive analysis, and even when there is demonstrable justification, controls should only be loosened in a step-wise manner (as described in section II.5).

The criteria for assuring the maintenance of defense in depth in risk-informed regulation are as follows. It is preferred, but not required that for each initiating event modeled, the plant response should have the following capabilities:

For anticipated operational occurrence (AOO) initiating events: the PRA-credited portion of the plant should withstand two active failures without core damage and three active failures without a large early release; and

For infrequent but severe design basis accidents defined as those with frequencies of 10^{-3} per year or smaller (e.g., large LOCA, main steam line break, etc): the PRA-credited portion of the plant should withstand one active failure without core damage and two active failures without large early release.

If the licensee does not satisfy the above criteria, the instances in which the plant falls short should be identified, and measures to

compensate for any such condition should be identified and discussed. For example, if an AOO and two active failures can lead to core damage, then measures need to be taken to keep the probabilities of these failures especially low.

Instances in which common cause failure (CCF) could compromise the redundancy credited in the above evaluations should be identified, and measures to prevent the occurrences of these CCF events should be identified and explained. The guideline in this case is that if all events in a minimal cutset belong to a common cause group, as defined in NUREG/CR-4780 (reference 8), or if all but one event belong to such a group, then CCF could compromise the redundancy credited. In the event that the cutset is entirely within a common cause group, the explanation of CCF prevention should be considered and substantive. In the event that the minimal cutset contains events outside the common cause group, the explanation can be based in part on measures taken to prevent those non-CCF events. Such cutsets are implicitly less threatening than cutsets capable of occurring as the result of a single common cause, and less discussion is required.

As part of the search for CCFs that could compromise defense in depth, sequence cutsets should be evaluated for potential systematic deterioration in multiple components (e.g., by aging) and for significant relaxation of requirements in multiple components. In this case, components of different types have to be considered together as long as they show up in the same cutset. The criteria for the treatment of potential multiple component failures is similar to that listed for CCFs (in the preceding paragraphs).

For purposes of these evaluations, maintenance actions and failures of certain operator actions (proceduralized actuation of system ...re counted as active failures. Post-accident recovery of failed equipment should not be counted in the above criteria. Post-accident recovery of failed equipment may be credited for purposes of assessing the overall plant risk profile, subject to guidance provided in NUREG-1602.

II.6.3 Criteria for Assuring Risk Balance

Regardless of the nominal value of a risk index such as CDF or LERF, it is undesirable for too large a fraction of this risk to be associated with a few elements. A more desirable risk profile is one in which no contributors are overly dominant. If one or a few elements clearly dominate risk, there will tend to be residual concerns about the modeling of that item (including uncertainty) or the effect on risk if it degraded, even if the absolute risk numbers are relatively low. Similarly, if one or a few accident sequences dominate, there might be residual concerns about modeling assumptions in that sequence, including initiator frequency, etc., in addition to possible concerns about the components that are important within that sequence. Therefore, one of the issues to be addressed in risk-informed changes is whether they create or exacerbate such a risk imbalance or whether plant resources and requirements can be redirected to balance risk contributors.

The suggested "SSC importance" test is whether any components become high risk contributors as the result of a risk-informed application (as defined as having a Fussell-Vesely importance of 0.05 or a Risk Achievement Worth of greater than 10). If an application causes any components to become a high risk contributor, then it should be shown either to result from a net safety benefit reallocating the relative importance of items, or shown to be a small change that happens to cross the boundaries as defined above.

A significant upward change in importance of an already high risk contributor should not be accepted except in the context of a net safety benefit, i.e., this should only be allowed if the component itself is not being relaxed but its importance is increasing because other contributors are being eliminated. Note that an already high contributor is also already a candidate for enhanced programmatic attention. If the proposed application increase its importance further, special consideration should be given to enhanced programmatic attention.

Similarly, a significant increase in importance should not be allowed for already-important sequences or initiators, unless the importance is increasing as a result of elimination of other contributors. If defense in depth requirements are met and a sequence is still excessively important, this may be a result of high unavailability of some elements in the model, and these may become candidates for increased programmatic attention.

Note that "risk balance" is not as important when the overall calculated risk is relatively low when compared to the allowed risk. However, risk balance is encouraged in all risk-informed applications.

II.6.4 Criteria for Consideration of Cumulative and Synergistic Effects from all Applications

The current policy intention is to relate an overall allowed change in risk to each plant's existing risk level. In approaching any given application, therefore, the flexibility available to any given plant is not only a function of where it started, but also a function of how much risk increase has taken place in preceding applications. The risk balance issue (sub section II.6.3) is also a part of this issue, because the intent of avoiding the creation of imbalance is meant to include not creating imbalance over several applications.

Beyond these cumulative effects, synergistic effects are also possible, not all of which would emerge from a point quantification of the PRA. For example, refer to Figure 1 which shows different influences on the availability of a given component. If conventional importance ranking approaches are employed, it would be expected that some low significant components will be relaxed under multiple applications. Referring to Figure 1, it can be seen for example that a given component might be a candidate for relaxation both of its QA (potentially affecting the failure rate) and of its test interval (potentially affecting fault exposure time). Failure rate and fault exposure time combine multiplicatively in the unavailability. If the effects of QA on failure rate could be quantified convincingly, this would be addressed explicitly under other figures of merit, but this cannot presently be assured. As a result, there is potential for different applications to lead to unintended synergistic effects on unavailability of a given component.

In addition to this, there is the potential for synergistic effects within a given minimal cutset, if different elements of the cutset are relaxed. Therefore, compensating SSCs (SSCs appearing in cutsets with SSCs directly affected by the application) must be reviewed to ensure that their performance is being adequately addressed in whatever assurance activities are applicable to that particular component type.

Cumulative effects are addressed by:

ensuring that each application is carried out with reference to a model that already reflects previous applications;

showing that the cumulative change is within the allowed increment; and

showing that the accumulation of applications has not created dominant contributors (unless this is a consequence of importance reallocation as a result of a net safety benefit).

Synergistic effects are addressed by:

showing that each component is relaxed under only one application; **OR**

explicitly identifying all components relaxed under multiple applications, arguing that the synergistic effects can be modeled correctly, and showing that the results of such modeling are acceptable with respect to the acceptance criteria.

II.6.5 Integration of Deterministic and Probabilistic Considerations

In general, the licensee's integration of deterministic and probabilistic considerations to form the basis for acceptance of a risk-informed application will be carried out by an Expert Panel. In order for this Expert Panel to be effective, a guideline detailing the decision process is required. This Expert Panel process has to be well-defined, systematic, repeatable, and scrutable. Scrutability implies that the process is technically defensible and is detailed enough to allow an independent party to reproduce the major results.

A well defined Expert Panel process should have the following (or similar) elements:

1) definition of objectives;
2) selection of experts;
3) identification of issues;
4) assembly and dissemination of information;
5) training of panel members including guidance for decision criteria;
6) panel deliberation;
7) post deliberation feedback;
8) treatment of disparate views and formulation of conclusions; and

9) documentation.

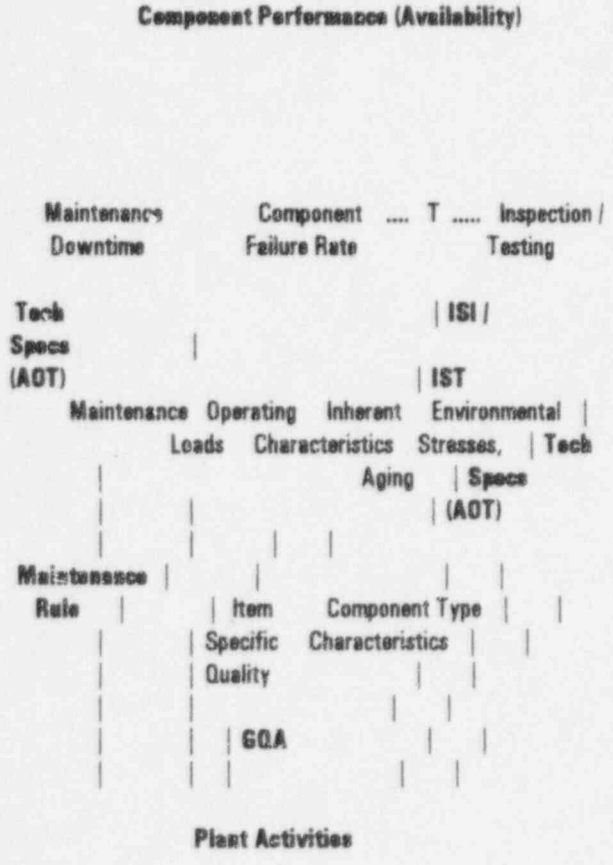
The panel members should have the appropriate qualifications, and acceptance of the determination of the Expert Panel includes the finding that the Expert Panel was advised of all the specific changes and relevant background information associated with the licensing action, and that the panel deliberated and approved each of the changes.

During deliberations, both probabilistic and deterministic considerations have to be taken into account. Potential limitations of the risk model have to be identified, discussed and resolved. SSCs that are affected by the proposed application but that are not modeled in the PRA have to be considered individually and evaluated based on a pre-defined and structured set of rules or criteria. Finally, the panel's results should be demonstrated to be robust to different plausible assumptions and analyses.

Additional criteria and review considerations relating to the Expert Panel are provided in Appendix B to this SRP which documents the requirements for qualifications of panel members and requirements for the verification of the consistency and accuracy of the panel's results and conclusions.

Figure 1

Effects of Plant Activities on Component Performance



III. REVIEW PROCEDURES

Specific procedures for reviews in the areas of IST, ISI, graded QA, and technical specifications are provided in the specific SRP chapters on those topics. General guidance for reviews in areas not treated in separate SRP sections is provided below.

III.1 General Guidance

When evaluating licensee requests for changes in regulatory requirements or positions, or previous licensee commitments, the reviewer should ensure that the submittal clearly identifies the original documented technical basis for the requirement, position, or commitment. This basis may be documented in an NRC order, a regulation, the statement of consideration for a rule, the statement of consideration for a rule, bases section of technical specifications, a regulatory guide, a formal staff position articulated in branch technical position (BTP), an industry code or standard, a vendor topical report, a staff safety evaluation report or inspection report, or in a generic communication such as a bulletin or generic letter, or a correspondence to or from a licensee. The reviewer should verify that the licensee has clearly and completely identified the technical concern that is at the crux of his relief request. It is only after this has been done that the staff can consider the issue in light of new information.

III.2 Evaluation of the Characterization of Change

The reviewer should verify that the effects of the proposed changes on PRA parameters are correctly characterized, i.e., verify that the effects of the changes on SSC reliability and unavailability or on operator actions are correctly accounted for. Where applicable, the modeling and quantification of the effects of the change should also be reviewed to ensure that the models are appropriate and that the results can be supported by plant and/or industry data.

Another element of the cause-effect relationship is the potential effect of the application on the total plant risk model. General guidance for the identification of PRA model elements that may be affected by an application can be obtained from Section 3.3 of the EPRI PSA Applications Guide (reference 4). This guidance, provided as a list of questions, will assist the reviewer in establishing a cause-effect relationship between the application and the PRA model. A supplemented list of these questions is tabulated in Table 1.

Table 1 (page 1 of 3)

Questions to Assist in Establishing the Cause-Effect Relationship

LEVEL 1 (INTERNAL EVENTS PRA)

Initiating Events

Does the application introduce consideration of new initiating events?
Does the application address changes that lead to a modification of the initiating event groups?
Does the application necessitate a reassessment of the frequencies of the initiating event groups?
Does the application increase the likelihood of a system failure that was bounded by an initiating event group to the extent that it needs to be considered explicitly?

Success Criteria

Does the application necessitate modification of the success criteria?
Does the modification of success criteria necessitate changes in other criteria, such as system interdependencies?

Event Trees

Does the application address an issue that can be associated with a particular branch, or branches on the event trees, and if so, is the branching structure adequate?
Does the application necessitate the introduction of new branches or top events to represent concerns not addressed in the event trees?
Does the application necessitate consideration of re-ordering branch points, i.e., does the application affect the sequence dependent failure analysis?

System Reliability Models

Does the application impact system design in such a way as to alter system reliability models?
Does the application impact the support functions of the system in such a way as to alter the dependencies in the model?
Does the application impact the system performance, and, if so, is that impact on the function obscured by conservative modeling techniques?

Parameter Data Base

Can the application be clearly associated with one or more of the basic event definitions, or does it necessitate new basic events?
Does the application necessitate a specialized probability model (e.g., time-dependent model, etc.)?
Does the application necessitate modifications to specific parameter values?
Does the application introduce new component failure modes?
Does the application effect the component mission times?
Does the application necessitate that the plant-specific (historical) data be taken into account, and can this be achieved easily by an update of the previous parameters?
Does the application involve a change which may impact parameter values, and do the present estimates reflect the current status of the plant with respect to what is to be changed?

Dependent Failure Analysis

Does the application introduce or suggest new common cause failure (CCF) contributions?
Does the application introduce new asymmetries that might create sub-groups within the CCF component groups?
Is the application likely to effect CCF probabilities?

Questions to Assist in Establishing the Cause-Effect Relationship

Human Reliability Analysis

Does the application involve a procedure change?
Does the application involve a new human action?
Does the application change the available time for human actions?
Does the application affect the human action dependency analysis?
Does the application eliminate or modify an existing human action?
Does the application introduce or modify dependencies between plant instrumentation and human actions?
Is the application concerned with events that have been screened from the model, either in whole or in part?
Does the application impact a particular performance shaping factor (PSF), or a group of PSFs, and are they explicitly addressed in the estimation approach? For example, if the issue is to address training, is training one of the PSFs used in the HRA?
Does success in the application hinge on incorporating the impact of changes in PSFs, and if so, do the current estimates reflect the current status of these PSFs?
Is it possible that the particular group of human error events that is affected by the change being analyzed has been truncated?
Does the change address new recovery actions?

Internal Flooding

Does the application affect the screening analysis, for example, does the application result in the location of redundant trains or components into the same flood zone?
Does the application introduce new flooding sources or increase existing potential flood inventories?
Does the application affect the status/availability of flood mitigation devices?
Does the application affect flood propagation pathways?
Does the application affect critical flood heights?

Quantification

Does the application change any of the basic event probabilities?
Does the application change relative magnitudes of probabilities?
Does the application only make probabilities smaller?
Is the new result needed in a short-time scale?
Does the application necessitate a change in the truncation limits for the model?
Does the application affect the "delete terms" used during the quantification process? (More specifically, does the application introduce new combinations of maintenance actions or operating modes that are deleted during the base case quantification process using the delete function?)
Does the application affect equipment that have been credited for operator recovery actions? Also, for recovery actions that credit inter-system or inter-unit cross ties, the effect on other systems or functions or on the operation of the other unit has to be considered and addressed.

Analysis of Results

Does the application necessitate an assessment of uncertainty, and is it to be qualitative or quantitative?
Are there uncertainties in the application that could be clarified by the application of sensitivity studies?
Does the application strategy necessitate an importance analysis to rank contributions?
Does the application necessitate that an importance, uncertainty, or sensitivity analysis of the base case PRA exist?

Plant Damage State Classification

Does the application impact the choice of parameters used to define plant damage states?
Does the Key Plant Damage States (KPDS) utilized adequately represent the results of the Level 1 analysis by including the plant damage states that have a significant frequency of occurrence?
Have those plant damage states that have been eliminated in this process been assigned to KPDSs of higher consequence (e.g. likelihood of Large Early Release)?

Table 1 (page 3 of 3)

Questions to Assist in Establishing the Cause-Effect Relationship

Level 2 (CONTAINMENT ANALYSIS PRA)

Have new containment failure modes identified by the application been addressed in the PRA? Are potential changes accounted for?
Are any dependencies among containment failure modes being changed?
Does the application involve mechanisms that could lead to containment bypass?
Does the application involve mechanisms that could cause failure of the containment is isolate?
Does the application directly affect the occurrence of any severe accident phenomena?
Does the application necessitate use of risk measures other than large, early release?
Does the application change equipment qualification to the point where it affects timing of equipment failure relative to containment failure?
Does the application affect core debris path to the sump / suppression pool (screen clogging) or to the other portions of the containment (direct containment heating)?
Does the selected source term categories adequately represent the revised Containment Event Tree (CET) endpoints? Are CET endpoint frequencies changed enough to affect the selection of the dominant/representative sequence(s) in the source term binning process?
Does the application affect the timing of release of radionuclides into the environment relative to the initiation of core melt? and relative to the time for vessel rupture?

LEVEL 3 (CONSEQUENCE ANALYSIS PRA)

Does the application necessitate detailed evacuee doses?
Are individual doses at specific locations needed for this application?
Are terrain features significant enough to impact local wind patterns?
Is evacuation or sheltering being considered as a mitigation measure?
Are long term doses a consideration in this application?

EXTERNAL EVENTS PRA (Hazard Analysis)

Will the changes introduce external hazards not previously evaluated?
Will the changes increase the intensity of existing hazards significantly?
Are design changes modifying the structural response of the plant being considered?
Does the change impact the availability and performance of necessary mitigation systems for an external hazard?
Does the application significantly modify the inputs to the plant model conditioned on the external event?
Are changes being requested for systems designed to mitigate against specific external events?
Does the application involve availability and performance of containment systems under the external hazard?

SHUTDOWN PRA

Will the changes affect the scheduling of outage activities?
Will the changes affect the ability of the operator to respond to shutdown events?
Will the application affect the reliability of equipment used for shutdown conditions?
Will the changes affect the availability of equipment or instrumentation used for contingency plans?

III.3 Evaluation of Deterministic Information

Reviewers should ensure that, for all risk-informed applications, licensing basis and other engineering considerations have been taken into account to supplement probabilistic arguments. To ensure that a proposed change does not unacceptably affect the licensing basis of the plant, deterministic evaluations should include evaluations of: preservation of the defense in depth philosophy; and general design criteria. In addition, pertinent engineering data and analysis, plant operating experience, potential compensatory measures, and a performance based feedback loop should also have been considered by the licensee.

The current licensing basis of the plant is defined as that collection of documents which forms the basis for granting the operating license and authorizing continued operation of the plant (see 10 CFR 54.3 for additional definition of "current licensing basis"). It includes, for example, the licensee's Technical Specifications, license conditions, commitments documented in the updated safety analysis report (USAR), commitments made in response to NRC generic letters and bulletins, conditions and analyses relied on in the NRC staff's safety analyses reports, etc. Application specific design basis documents and relevant plant licensing commitments are also important. The licensing basis of the plant also documents how the licensee satisfies certain basic regulatory requirements such as diversity, redundancy, defense in depth, and the General Design Criteria.

As part of the evaluation of deterministic information, NRC review should include a check of engineering evaluations which may be needed to support the PRA especially in areas where the current licensing basis may be relaxed (an example being the determination of success criteria). Reviewers should also verify and validate calculations and data used to model the effects of the risk-informed applications on the affected SSCs and on PRA models, assumptions and parameters (cause-effect relationships).

Finally, the reviewer should verify that the deterministic considerations used to supplement PRA results (e.g., information used to determine SSC importances, or information used to evaluate plant systems or components which are not modeled in PRA) are applied comprehensively and correctly. Among the non-PRA sources of information that should be examined to support the evaluation of safety significance are the safety insights developed in licensing documents including the Final Safety Analysis Report, the bases for Technical Specifications such as Limiting Conditions for Operation (LCOs), Allowed Outage Times (AOTs), and Surveillance Requirements (SRs). Finally, where available, plant specific data and operational information should be factored into all safety determinations.

Engineering Data and Analysis

In many cases licensees will cite new data from plant tests or research projects, or analysis with models based on new data to support their proposal. The following examples illustrate situations in which data and analysis can be used effectively to support relief requests:

To show that a phenomena of concern cannot occur or is much less likely to occur than originally thought;

To show that the amount of safety margin in the design is significantly greater than that which was assumed when the requirement or position was imposed;

To show that time available for operator actions is much greater than originally assumed.

The reviewer's primary objective is to verify the relevance and acceptability of this new information with respect to the relief request. Data which applies directly to the original technical concern should be applied in the decision process. Depending on the circumstances, additional specific guidance in the cognizant review branch may be available for reviewing the quality and acceptability of the data. However, in all cases, the data or analysis must be clearly applicable to the plant and specific circumstances to which it is being applied.

Operating Experience

When conducting reviews of PRA assessments, reviewers should consider the way in which the issues at hand are reflected in operational data. A substantial amount of engineering data is available for use in evaluating assumptions regarding initiating events, component and system reliability and common cause failure mechanisms. AEOD gathers data from several sources, evaluates the data and compiles it in substantial number of reports. Currently available reports are listed in Reference 7.

Useful insights from plant specific operating experience can also be obtained from inspections that follow incidents at the facility, including NRC incident investigation and augmented team inspections, INPO incident assessments documented in significant operating

event reports, licensee follow-up investigations and routine inspections by NRC resident inspectors. Inspection results can provide valuable qualitative insights in areas such as human performance, management controls, adequacy of procedures and root causes of events which are often difficult to treat with precision in a PRA.

Compensatory Measures

Compensatory measures at the plant site which reduce risk can be taken to offset incompleteness or uncertainties in the deterministic or probabilistic analysis that defines available safety margin. Compensatory measures can also be used to offset a quantifiable increase in risk with a non-quantifiable but expected improvements in safety. Such measures may be taken voluntarily by licensees or may be required by the NRC as conditions of the license, temporary changes to technical specifications, or by order. Examples of such measures include: special inspections or tests; enhanced condition monitoring; moratoriums or prohibitions of site activities during specified periods of vulnerability; temporary increase in staffing level, special training for staff or contractors; procurement and staging of portable back-up safety equipment (e.g. skid-mounted diesel generator) and development of procedures and training for use of such equipment. Compensatory measures should be given significant weight in the decision process for reviews of risk-informed applications when:

1) they are keyed directly to a critical part of the analysis that carries uncertainty (e.g. enhance training and procedures when uncertainty in human performance is an important factor);

2) they qualitatively offset a quantitative risk increase; or

3) the measures are required by the license and controlled by explicit licensee procedure or subject to inspection by the NRC.

III.4 Evaluation of Probabilistic Information

Reviewers should ensure that PRA related information submitted by a licensee for applications in risk-informed regulation includes: 1) a characterization of the change analysis; 2) a justification for the scope and level of detail of the PRA; 3) a discussion of the numerical results and risk insights obtained from the analysis and a comparison of the results to the decision criteria specified in the Regulatory Guide; and 4) the results of the licensee's independent peer review of the PRA in the form of the peer review team's final report.

In the review of risk-informed submittals, it is anticipated that these submittals can be categorized with respect to the expected level of sophistication in the PRA analysis. For example, the justification for continued operation (JCO) proposed by licensees in light of non-conforming conditions and the technical review of the bases for notices of enforcement discretion (NOED) are expected to be relatively simple applications in terms of PRA analysis required, and therefore these applications will require less in terms of PRA quality, scope and level of detail. However, for this PRA to be used, it must be shown to adequately bound the risk impact of the contributors associated with the application. Conversely, changes to plant specific technical specification allowed outage times and surveillance test intervals, safety evaluations regarding plant specific design issues and plant specific backfit evaluations, and review of a design-specific PRA submitted per section 10 CFR 52.47 of the regulations are examples of applications that will require detailed PRA evaluations and will be subject to a higher level of PRA quality, scope, and level of detail.

For each submittal the licensee will have to justify, and the staff reviewer will have to verify that the scope, level of detail and quality of PRA is sufficient to support the risk analysis. The determination of acceptable PRA scope and level of detail should be based, in large part, on the cause-effect relationships established in the characterization of the problem (see section III.2). The PRA quality will have to be consistent with that specified in NUREG-1602 for the portions of the analysis that is affected by the application.

III.4.1 Required Scope of Analysis

The overall scope of a PRA is characterized in terms of three attributes:

1. Which operational modes are considered, e.g., full power, low power, transitional states, and shutdown;

2. Which initiating events are considered, e.g., internal and external events; and

3. What level of analysis is performed, i.e., level 1 (core damage frequency), level 2 (containment response and /or source term), and level 3 (offsite consequences).

The selection of PRA scope will be guided by the nature of the technical issues being addressed with the PRA. Guidelines for selecting the scope are provided in the application specific regulatory guides and standard review plans. The following general guidance is provided for the use of staff reviewers for cases in which there is no application specific SRP.

The reviewer should verify that the licensee has considered all possible operating modes and initiating events that could be affected by the proposed application.

The reviewer should verify that the licensee's approach for selecting and evaluating applicable initiating events and operating modes is similar to those accepted by the staff in reviews of similar issues for similar plants. Unexplained differences should be brought to the licensee for explanation.

A Level 1 PRA analysis is usually required for most applications. A Level 2 study is recommended for applications which might have an impact on containment systems or containment isolation probability. A Level 3 PRA is recommended for emergency response and planning applications or when cost-benefit evaluations (person-rem per dollar) are needed. When the Level 2 or Level 3 studies are not available, engineering justification and bounding evaluations are acceptable if they are comprehensive and have sufficient rationale.

Unless an application deals with SSCs that are needed solely for low power and shutdown operations, a full power PRA is required. When the SSCs in question are needed for more than just full power operations, low power and shutdown PRAs are also recommended. Applications that compare risks at full power operation to those in other operating modes (e.g., on-line maintenance, or modifications of technical specification requirements) should also include low power and shutdown PRAs. In the absence of these PRAs, plant response capability during low power and shutdown operating state has to be addressed and satisfied. This is discussed later in this section.

Direct risk insights (risk ranking, increase in risk, etc.) cannot be obtained from initiators that have been screened out. External events analyses that depend largely on screening techniques fall into this category. In addition, it cannot be assumed that risk insights from the external initiators are similar to those for the internal initiators. External events could result in initiators (or relative importances of the different initiators) that are different from those from internal events, and therefore, insights and conclusions could be skewed by this different mix of initiators. Appendix B (section B.4) discusses more in detail the review procedures for screened-out events.

When licensee PRAs do not treat all plant operational modes and/or all initiators, the reviewer has to determine the acceptability of proposed application without comprehensive PRA coverage. For each instance (combination of mode/initiator type) in which the PRA does not analyze plant response, the reviewer has to establish that the licensee has provided arguments for a plant response capability. If an adequate plant response capability exists without resort to SSCs affected by the application, then the issue of scope is considered to be resolved satisfactorily. If credit for affected SSCs is needed, then the reviewer establishes that the defense in depth criteria specified in section II.6.2 are satisfactorily passed and that vulnerabilities (as defined in section II.6.3) are not introduced. In addition, the reviewer verifies that the bounding risk from the unanalyzed portions of the PRA are calculated in a conservative fashion, and is consistent with risks from similar plants.

III.4.2 Required Level of Detail

For all components affected by the application, the reviewer should verify that the models are detailed enough to account for important system and operator dependencies. A check of the licensee failure modes and effects analysis and a review of plant operating and emergency procedures will be useful for this purpose.

In addition, the reviewer should determine that risk insights obtained from a PRA for a particular SSC is consistent with the level of detail of modeling for that SSC. If it can be determined that a SSC can be attributable to a PRA basic event on a one-to-one basis and that the cause-effects of the application can be reflected on that basic event, then risk insights from the application can be directly obtained from the PRA for that SSC. Otherwise, PRA risk insights have to be supplemented by other engineering and operational information that can

be integrated via an expert panel process.

Specifically, the level of detail in the modeling of each SSC can be used to determine the following:

If the SSCs are modeled at the basic event level, i.e., each SSC is represented by a basic event (or sometimes, more than one if different failure modes are modeled), risk insights from the PRA can be directly applied to the component modeled as long as the effects of the change is modeled correctly.

If the SSCs are included within the boundaries of other components (e.g., the governor and throttle valves being included in the pump boundary); or if they are included in "black boxes" or modules within the PRA model; or they are modeled as part of the calculation of human error probabilities in recovery actions, risk insights from the PRA can be applied if the effects of the application can be mapped onto the events (e.g., modules, HEPs, etc.) in question. In these cases it should be noted that the mapping is relatively simple if the event is ORed with the other module or HEP events. However, if the logic involves AND gates, caution is warranted.

If the SSCs are only implicitly modeled (e.g., omitted from the model because of inherent reliability), or if they are not modeled at all (because no credit for the SSCs were taken for accident mitigation), risk insights from the PRA can only be applied after evaluation by the Expert Panel. Requirements and review of this process is provided in Appendix B of this SRP.

III.4.3 PRA Quality

The quality required of a PRA for risk-informed regulation is defined in NUREG-1602 (reference 5) which also provides guidelines to treat the quality of the process used to conduct the PRA study, the quality of the technical analysis performed and the quality of the documentation of the PRA.

Quality in the Process for Conducting a PRA

In accordance with Appendix B to 10 CFR Part 50, licensees should have a formal program for applying PRA in safety-related activities that affect systems, structures and components that prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. Periodic staff review of this program is accomplished through an audit or inspection. Guidelines for conducting the inspection are provided in section xx.yy of the NRC Inspection Manual.

Quality in the Technical Analysis

Quality is assured in the licensee's technical analysis by subjecting the completed analysis for independent technical peer review. Guidelines for conducting such a review are given in NUREG-1602. In accordance with those guidelines, the peer review team formally documents the results of their review in a report which is available to the NRC staff for audit. The following factors should be considered in determining the need for staff review of the peer review report.

Staff audits of the licensees process for conducting a PRA have identified practices which could affect the quality of the technical analysis detrimentally;

Results of the licensee's analysis submitted in support of a licensing action are in some way counter-intuitive or inconsistent with results for similar plants on similar issues (For each application, licensees should have documented that a review of available information has been performed to identify potential inconsistencies in results and conclusions);

The process the licensee used to identify the safety significance of the SSCs modeled in the PRA does not have the ability to appropriately identify the significance of all the SSCs for the particular application;

The PRA is being applied to an issue of potentially high risk impact that warrants a more comprehensive staff review;

The licensee's analysis is part of a pilot application of PRA in a regulatory activity;

The PRA includes new methods that are unfamiliar to the staff.

Review of PRA Quality

As stated above, detailed findings on PRA technical adequacy can be based on an NRC staff audit of the licensee-sponsored external peer review. However, for each application area, specific findings will have to be made regarding the quality of the PRA. These findings should be based on a "focussed-scope" staff review which will concentrate on application specific attributes of the PRA.

For any application, the reviewer must reach a finding of reasonable assurance of the following, based either on his/her own review, or an audit of a licensee sponsored review:

Comprehensive Set of Initiating Events: Within the PRA's scope, a suitable set of initiating events has been analyzed. The process for identification of initiating events was appropriately thorough; it made appropriate use of reviews of operating experience and plant design information. In particular, a systematic search for plant-specific initiating events was carried out. All support systems that are functionally linked to front-line systems were examined for initiating event potential. Initiators resulting from internal flooding, fires and other external events was included in this search.

Detailed and Complete Logic Modeling: Functional logic modeling of plant response is appropriate. As far as can be determined consistent with the current state of the art, the modeling of scenarios is complete in the sense that for each initiating event modeled, probabilistically significant scenarios capable of leading to core damage and/or large release are represented qualitatively in the scenario model, and others have been screened out on the basis of documented considerations. Scenarios were modeled in sufficient detail to support findings regarding importance of systems, structures, components, and operator errors. The logic of the scenario models is consistent with the analysis of the mission success criteria.

Comprehensive Search for System Interactions: An appropriate search for system interactions has been carried out, and the results reflected in the modeling. This addresses primarily phenomena that couple failures of nominally independent events, such as damage to co-located SSCs from a single event such as fire or flood.

Mission Success Analysis: Physical analysis to support the formulation of mission success criteria was appropriate. Controlled versions of generally accepted thermal-hydraulic models were employed. Within each credited success path, the most limiting equipment configuration credited as "successful" was analyzed and shown to provide adequate performance with sufficient margin to justify describing the path as successful. The sequences for which such margin is lacking have been binned into plant damage states characterized as marginal.

Accident Sequence Binning: The binning of accident sequences is appropriate; it supports the distinctions necessary to permit quantification of appropriate figures of merit, such as CDF and LERF. The analytical basis for binning of sequences is firmly established.

Appropriate Use of Generic and Plant Specific Data: PRA basic event probabilities have been modeled appropriately especially for components affected by the application. Specific component failure modes are imputed to each basic failure event. The corresponding fault exposure times are properly linked to programmatic activities (IST, ISI, etc.). The corresponding failure rates have been quantified appropriately in light of generic data, plant-specific data, plant QA, and the nature of the component's operating environment (loads, frequency of cycling, environment, etc.). Maintenance unavailability has been modeled appropriately using plant experience.

Adequate Treatment of Human Factors: Human factors have been treated appropriately for the specific application. Significant human actions have been systematically identified, and failure probabilities have been quantified according to state-of-the-art methods as discussed in NUREG-1602. Coupling between human actions has been considered. Where credit taken for post-initiator recovery actions has had a significant effect on the conclusions for the specific application, licensees have committed to ensuring the viability of those recovery actions, to a degree commensurate with their difficulty and their significance.

As part of the determination of PRA quality, there should be a staff finding that the licensee's configuration control of the PRA will provide ongoing reasonable assurance that the PRA will continue to represent the plant. The following should be included as part of the review:

There is adequate commitment to maintain the PRA to reflect current plant status (including current procedures as well as current physical configuration) and to incorporate new information (including, but not restricted to, failure data, updated thermal hydraulic modeling, etc.). When new information leads to modification of analysis whose results were previously applied to justify modifications, this will be brought to the attention of NRC staff.

Calculations to support PRA applications are performed in a controlled fashion. Sensitivity studies are performed to characterize the effect, if any, of such analytical shortcuts as truncation, if this applies to the subject analysis. For each application, a designated controlled version of the plant model is used, and a designated controlled set of parameter inputs (e.g., basic event probabilities) is used. The licensee warrants, and external peer review concurs, that applications will not be adversely affected by artifacts such as truncation.

Appendix A of this SRP provides a more detailed discussion of several issues important to the review of probabilistic evaluations performed as part of risk-informed regulation.

III.4.4 Evaluation of Model Uncertainties

If a risk-informed application contends that the estimated risk change due to the proposed changes is conservative, then the reviewer should confirm that the models and data assumptions used do indeed produce a demonstrably conservative estimate which is likely to be near the upper bound.

If the calculated risk change due to an application is large when compared to the allowed risk change and is a best estimate value, then the reviewer has to establish that uncertainty is addressed for the change. This argument should appropriately include data and model uncertainties. The licensee may be able to argue without explicit propagation that the uncertainty is small compared to the margin between the allowable change and the estimated change. In some cases, sensitivity studies could be used to demonstrate the robustness of results to analysis data and models used.

In the review of the analysis of uncertainties, the reviewer should:

review the types and sources of uncertainty that have been identified by the licensee, and how the uncertainties have been characterized, and determine whether this characterization of uncertainty is consistent with the state-of-the-art as defined in NUREG-1602;

review how these uncertainties are reflected in the results of the PRA analysis, and determine whether the use of the mean is an adequate representation of overall uncertainty. (If an uncertainty analysis has not been performed, then a point estimate may be adequate if it can be demonstrated, from an inspection of the contributing cutsets, that it is sufficiently close to the mean);

identify whether the results of the analysis, whether they are presented in terms of absolute risk measures or in terms of SSC ranking or prioritization, are strongly impacted by the specific models or assumptions adopted for the assessment of important elements of the PRA, and whether the sensitivity analyses that have been performed (if any) are sufficient to address the most significant state-of-the-art uncertainties with respect to these elements, using NUREG-1602 as an input. (Care should be taken when the characterization of a model uncertainty is such that the results fall into a bimodal or multi modal distribution, and one or more of the modes exceeds the allowed goal. The assessment of the results then has to be based on an assessment of the significance of the hypotheses associated with those modes that exceed the goal);

determine whether the limitations in scope of the PRA, and other completeness issues have been addressed adequately by either limitation of the scope of the application, or by a demonstration that the impact of the change on the unanalyzed portion of the risk is bounded or can be neglected.

III.5 Evaluation of the Implementation and Monitoring Strategies

The reviewer should evaluate the implementation and monitoring strategies based on findings of the deterministic and probabilistic engineering evaluations. When the proposal is for a phased implementation for different SSC groups, the basis for the phasing for each SSC group should be justified.

To detect degradation of SSCs that are affected by the change in regulation, monitoring strategies should involve the evaluation of the performance of these SSCs over a period of time. This monitoring should be based on the performance (reliability or unavailability) and key modeling assumptions allocated to SSCs in the risk model used to support the proposed change in regulation. Monitoring that is performed as part of the Maintenance Rule implementation can be used in cases where the SSCs affected by the application are also covered under the Maintenance Rule.

If degradation is found, then the SSCs should either be refurbished, replaced, or tested/inspected more often (or a combination of these initiatives). The selected action should be based on the perceived nature of the degradation, whether it is generic, age related, etc. The reviewer should evaluate if the information gathered during monitoring activities is extensive enough to provide a timely indication of component degradation. Since many components are inherently quite reliable, the limited tests on a limited number of similar components may not provide adequate data, especially for newer plants where aging effects may not be detected until the proposed program is fully in place (and the advantages of a staggered implementation is lost). One approach to ameliorate this concern is to require that the performance of similar SSCs at other plants, with a range of operating times, be also monitored to provide a statistically significant data base over a range of component ages. Such a program would be expected to provide a much better chance of early detection of SSC reliability degradation.

A review (or evaluation) of the impact on plant risk and SSC functionality, reliability and availability given the proposed implementation and monitoring plan should also be carried out. The benefits from the implementation and monitoring programs should be balanced against any negative impact on risk.

Finally, the reviewer should also look at the criteria to be applied in deciding what actions are to be taken in cases where performance falls below that predicted by the supporting evaluations. Corrective action procedures should be in place before implementation of the proposed program.

III.6 Evaluation of the Integrated Decision Making Process

Review findings in this step will fall into two general areas: findings on the change acceptance (numerical risk impact, defense in depth, risk balance, and cumulative and synergistic effects) and findings on the integration of deterministic and probabilistic considerations. Each of these areas is discussed in the sub-sections below.

III.6.1 Evaluation of the Acceptance of Risk Impact

*** **TO BE COMPLETED** - this will depend on what Appendix B of the final Reg Guide DG-1061 will say ***

III.6.2 Evaluation of Defense in Depth

Defense in depth is an approach to safety according to which accidents are prevented through redundancy and diversity: plants are designed and operated in such a manner that accidents that threaten public health can occur only if multiple (redundant) and diverse pieces of equipment (or human actions) fail. Release of radioactive materials from the reactor to the environment is prevented by successive and mutually independent passive barriers: fuel cladding, reactor coolant pressure boundary, and containment structure. These barriers, together with an imposed exclusion area and emergency preparedness, are the essential elements of defense in depth at modern light water reactors. Given these multiple barriers, assurance of safety is provided by application of deterministic safety criteria for the performance of each barrier, and design and operation of systems (lines of defense) to support the functional performance of each barrier.

The following objectives therefore promote safety within a defense in depth concept:

1) Prevent undue (excessively frequent) challenges to the integrity of the barriers,

2) Prevent failure of each barrier when it is challenged,

3) Assure independence among barriers (prevent failure of one barrier as a direct consequence of failure of another barrier), and

4) Provide for prompt and appropriate response upon the failure of one or more barriers.

5) Provide overall redundancy and diversity in the barriers which is sufficient to provide significant probabilistic margin to the Safety Goals.

The risk-informed regulatory process is not expected to result in any qualitative changes in the major barriers: satisfaction of various General Design Criteria, and compliance with NRC rules such as 10 CFR Part 50.46, are not expected to be affected by this process. However, requirements effecting the supporting systems could be affected as a result of risk-informed regulation. It is important for the reviewers to identify the nature of this impact and its relation to safety in terms of its impact on the reliabilities of barriers. Since PRAs play a fundamental role in such regulatory approaches, the relationship of PRA output to the lines of defense needs to be determined.

Relationship Between PRA and Defense In Depth

PRAs provide both quantitative and qualitative results. The PRA quantitative results on core damage frequency, containment failure probabilities, frequency of various release categories, and finally public risk can be compared to the numerical acceptance criteria to show the effects on safety as a result of proposed changes. These quantitative results are strongly influenced by defense in depth, and vice versa, but some PRA estimates of accident frequencies may be low despite relative lack of redundancy, etc. Qualitative PRA results, i.e., the accident sequence minimal cutsets, show what combinations of passive and active failures would cause core damage or a radioactivity release, and thereby reflect directly on defense in depth. Qualitative results do not reflect accident frequency except implicitly, through event classification (e.g., some initiators are AOOs, and some basic events are active failures); but they show certain properties of system designs, unobscured by at least some of the uncertainties associated with quantification.

Provided that the PRA is technically sound, as described in NUREG-1602, the effective redundancy and diversity of a design show up qualitatively in the minimal cutsets. If many failures are required in order to cause the top events (core damage and large release), i.e., if all the minimal cutsets comprise many failures, then the effective redundancy is high. If no CCF event can cause the top events, i.e., if no minimal cutset consists entirely of events from a single common cause group, such as "MOV fails to open", and if no modeled CCF event is a single CCF element cutset, then the design incorporates at least some diversity. Each event appearing in each minimal cutset is, in general, targeted by programmatic activities aimed at promoting the reliability of the associated SSC, i.e., preventing the occurrence of that failure event. Specific activities that are important in maintaining reliability of a component are: inservice testing, inservice inspection, other periodic surveillance required by Technical Specifications, quality assurance, and maintenance.

In order to maintain defense in depth, it is essential to assure that multiple elements of important cutsets are targeted by at least some activities aimed at promoting assurance of the performance of the corresponding SSC. The qualitative acceptance criteria articulated in sub section II.6.2 are intended to assure that some programmatic attention is paid to sufficient elements of each accident sequence cutset, even if a point estimate calculation for a system with less than customary redundancy and diversity appears to satisfy the numerical guidelines on CDF and LERF. This approach comports with current licensing review practice for DBAs and AOOs.

Review Guidance

The reviewer should verify that:

the licensee explicitly characterizes the standing of the plant with respect to the defense in depth criteria provided in sub section II.6.2.

all elements counted against the criteria called out above receive at least some programmatic attention, and this programmatic

attention is commensurate with the quantitative (functional reliability/availability) performance level associated with that element.

minimal cutsets that fall short of the above criteria are identified and discussed; special measures are taken to prevent the events occurring in those cutsets.

It is expected that SSCs that are candidates for reduced activities will not be SSCs that appear in cutsets that do not satisfy the above criteria. That is, where redundancy and/or diversity are already marginal, it is arguably inappropriate to reduce the level of activities aimed at ensuring SSC performance, unless the activities are shown to have little or no effect on SSC performance. It is possible, however, that compensating or alternative activities could provide assurance of SSC performance. The point is not to completely relax the defense in depth posture at points in the design that are relative safety bottlenecks.

Inevitably, SSCs that are candidates for relaxation will appear in cutsets that exactly satisfy the criteria. Some reduction of activities on these SSCs can be tolerated, provided that frequency guidelines are satisfied, outliers are not created or exacerbated, there remains a basis for the credit taken for SSC performance, and that proposed relaxations do not create vulnerabilities to CCF. Reviewers are given further guidance on verifying defense in depth in application-specific guidance.

III.6.3 Evaluation of the Required Risk Balance

Importance measures are one tool for performing the check of risk balance on a component level. If no items become high risk contributors (i.e., have Fussell-Vesely values move above 0.05 or RAW values move above 10), then the test is passed. However, it is easy for a measure that causes a risk decrease to cause an increase in the relative importance of some elements, so relative importance measures alone cannot be the sole criterion. The preferred approach is therefore to apply the importance test first, and if it is passed, then provisionally conclude that the risk imbalance test is passed. If the importance measure test is not passed, then an explanation should be provided as to why the importance increases are acceptable. Perhaps they could be the mathematical side effect of an absolute decrease in calculated risk, or perhaps a few elements actually became more important because cutsets in which they appear became more probable. In the latter case, a justification would need to be offered along the following lines: either the associated changes in importance are small, and simply happened to cross thresholds above, or there are safety benefits that offset the increased sensitivity of risk to these elements (such as a net improvement in safety).

These considerations apply both at the component level and at the sequence level. If either initiating events or individual accident sequences become important as a result of application changes (as defined in sub section II.6.3), this should be addressed as indicated above. If the conditional core damage probability associated with a particular initiating event becomes significant, then this should likewise be addressed. This requirement is closely associated with defense in depth requirements articulated separately in sub section II.6.2.

The reviewer should verify that the licensee warrants that no components become high risk contributors as a result of the application, or that the licensee furnishes adequate explanations (net safety benefit, etc.) for changes that occur. If initiators or sequences substantially increase in importance, the reviewer verifies that the licensee warrants that this is a result of other contributors having been eliminated.

Formally, it is also necessary to address this issue for areas in which PRA information is not available, and a qualitative, success-path-based surrogate has to be used. In such a case, the importance guidelines indicated above cannot be applied. Reliance is then being placed on the defense in depth guidance.

III.6.4 Evaluation of the Cumulative and Synergistic Effects from all Applications

Synergistic effects on a given element can be addressed by showing that the basic event model adequately reflects the effects of programmatic activities and that the calculated unavailability, propagated through the PRA, is consistent with needed performance, with regard to high-level risk indices, risk balance, and defense in depth.

However, it is more straight-forward simply to avoid relaxing multiple programmatic requirements on a given component, unless demonstrable justification is provided that the risk contribution from the component is negligible for all conditions covered by the set of requirements. For example, if IST is relaxed on a given component, it would be preferable not to relax QA as well, unless good arguments are given for allowing this.

The reviewer should verify that the current application starts with a model that has been accepted as adequately reflecting all previous applications. The reviewer verifies that the cumulative change over all applications to date is consistent with the gross allowable change determined from the risk profile before any applications were initiated. This applies both to high-level risk indices and to component importance measure changes.

The reviewer verifies that the Expert Panel has addressed the issue of synergistic effects along lines indicated above and in section II.6.4.

III.6.5 Integration of Deterministic and Probabilistic Considerations

For many risk-informed applications, licensees will utilize the review of a panel of experts to supplement the quantitative analysis provided by the PRA. These experts will be used to address potential limitations of the PRA models and conclusions. This includes cases where PRA models are incomplete, i.e., in cases where the scope of certain applications include components that are not modeled in the PRA and therefore the risk significance of the component cannot be quantified. Expert Panels are also important in cases where the nature of the application does not allow for precise quantification of the performance of SSCs before and after proposed changes or where the use of rigorous data analyses and/or reliability engineering models is not practical or possible. For each of these cases, the Expert Panel will be used to justify the relaxation or removal of current regulations based on bounding analyses to show both small changes in risk and small changes in expected performance.

As part of the qualitative risk-informed process, the reviewer should verify that the Expert Panel has addressed the following questions for each SSC that has been proposed as a candidate for relaxation or removal of current requirements:

1) Is the component a part of a system that acts as a barrier to fission product release during severe accidents?

2) Can the system perform a support function to a safety function or complement a safety function?

3) Can the SSC support operator actions credited in PRAs for either procedural or recovery actions either because they are an essential part of the recovery process, or because they provide important information?

4) Can the failure of the SSC result in the eventual occurrence of a PRA initiating event?

5) Can the failure of the SSC result in unintentional releases of radioactive material even in the absence of severe accident conditions?

6) Is the SSC currently included in the scope of current regulatory requirements?

If the answer to all the above questions is "No", an SSC can be qualitatively ranked as low risk contributor and can be a candidate for reduced regulation. If the answers to any of the above questions is "Yes", or if SSC performance is difficult to quantify, the Expert Panel should have used a qualitative evaluation process to determine the impact of relaxing requirements on equipment reliability / performance. This evaluation should include an identification of those failure modes for which the failure rate may increase, and the failure modes for which detection could become more difficult. The reviewer should then verify that the following justifications (or similar) were provided by the Expert Panel:

1) a qualitative discussion and historical evidence why these failure modes may be unlikely to occur;

2) a qualitative engineering discussion on how such failure modes could be detected in a timely fashion;

3) a discussion on what other requirements may be useful to control such failure rate increases; and

4) a qualitative engineering discussion on why relaxing the requirements may have minimum impact on the failure rate increase.

Regulatory Guide DG-1061 provides general guidance for use by licensees in establishing an Expert Panel, including guidance on the composition of the panel, qualifications of panel members and procedures for conducting review activities. Additional specific guidance regarding the work of Expert Panels is also provided in the individual topical regulatory guides and Standard Review Plan sections. In general, staff reviews of Expert Panel deliberations should confirm that:

1) the panel includes experienced individuals with demonstrated skills and knowledge in relevant engineering disciplines (depending on the issues under review), plant procedures and operations, system knowledge including history, system response, and dependencies, operator training and response, probabilistic risk assessment and regulatory guidance;

2) the panel uses a sound and systematic process for establishing the scope and depth of their review, and the process (including guidelines and criteria) is documented;

3) the evaluation process is capable of identifying important areas not modeled in the PRA, assumptions in the PRA (e.g., success criteria) that are not consistent with system design, operational practice, plant operating experience or the latest research;

4) the panel had the benefit of well organized and documented input from the PRA and deterministic evaluations, and that all items in the evaluation were specifically addressed and resolved by the panel;

5) the deliberations and conclusions of the panel are formally documented for staff review in a format comparable to that given in NUREG-1602 and the technical reasoning used to reach a conclusion should be defensible and should be openly displayed for review and scrutiny;

6) the rationale for the results is auditable;

7) the results are shown to be robust in terms of the possible range of conclusions that could be arrived at from the distribution of PRA and deterministic inputs;

8) potential built-in biases have been addressed since the experts are generally obtained from in-house sources;

9) when aggregating expert judgements, the process would not mask or destroy information (individual judgements) that might be important for regulatory decisions. All dissenting points of view should have been documented.

The staff should review the panel's contribution to the decision-making process. Emphasis should be placed on those aspects of the issue that have not been treated in the PRA or carry significant uncertainty in their treatment.

For some applications such as graded QA or ISI where the PRA covers only a small fraction of the affected SSCs, a working group including both PRA experts and other personnel with extensive competence in the area under consideration may be needed to more fully present the safety case to the Expert Panel. The staff reviews of the working group will be similar to the review of the Expert Panel, but more emphasis will be placed on the specific expertise and findings of the working group members by the lead NRR technical branch.

A more detailed discussion of the review of the expert panel process is included in Appendix B to this SRP.

IV. EVALUATION FINDINGS

The results of a reviewer's evaluation should reflect a consistent and scrutable integration of the probabilistic considerations and traditional deterministic considerations provided by the licensee or applicant and developed independently by the reviewer. To make a finding of acceptability the reviewer will generally need to show that in light of a small or non-existent increase in risk and a reduced level of conservatism, safety margins remain adequate. Findings of acceptability must be supported with logical bases built from an evaluation of the considerations given in section III. Differences between the results of probabilistic and deterministic evaluations must be reconciled to achieve acceptable results in both risk and engineering conditions, prior to making a finding of acceptability.

The reviewer verifies that sufficient information is provided in accordance with the requirements of this SRP and that the evaluation supports conclusions as specified in the sections below, to be included in the staff's safety evaluation report.

IV.1 General

The plant's current licensing basis and actual operating condition and practices are properly reflected in the PRA models.

Results from the risk analysis and from those deterministic evaluations yield conclusions that are consistent with respect to safety importance;

When risk insights are used to quantify conservatism in the original licensing basis analysis, it was shown that the original intent of the requirement is still being satisfied;

PRA results and conclusions are shown to be robust in terms of the analysis inputs, assumptions and uncertainties;

When lack of completeness or uncertainties in the PRA models affects the risk-informed decision making, applicable deterministic information or compensatory actions were used to assure a conservative outcome;

Net changes in risk do not exceed the criteria specified in Appendix B of Reg Guide DG-1061;

Where applicable, the process used to justify relaxation in requirements was also used to identify areas where tightened controls would improve safety.

IV.2 Characterization of Change

Cause-effect relationships have been identified to adequately link the application with the PRA.

The proposed risk models can effectively evaluate or realistically bound the effects of the proposed change;

IV.3 Deterministic Evaluations

Proposed changes were reviewed with regard to the current licensing basis, and the changes do not unacceptably

affect the intent of the licensing basis;

Information from engineering analyses, operational experience, plant-specific performance history have been factored into the decision process.

IV.4 Probabilistic Evaluations

IV.4.1 Scope of Analysis

The licensee's PRA satisfactorily addresses all mode/initiator combinations, **OR**

The licensee's PRA does not analyze the following mode/initiator type combinations. [List combinations] In each instance, the licensee has:

1) satisfactorily identified significant plant challenges, **and**

2) identified a complement of plant response strategies that possesses sufficient redundancy and diversity to provide suitable assurance of successful plant response, **and**

3) shown that either:

   a) the proposed changes do not affect this response capability, **or**

   b) the proposed changes leave intact sufficient response capability, **or**

   c) the proposed changes do not unacceptably degrade this response capability.

   and

4) ensured that all elements of the plant response capability are subject to programmatic activities to assure suitable performance.

IV.4.2 Level of Detail

The PRA is detailed enough to account for all important system and operator dependencies;

Risk insights are consistent with the level of detail modeled in the PRA.

IV.4.3 Quality of the PRA

There is reasonable assurance of PRA adequacy as shown by the licensee peer review process and by a focussed scope application-specific review by the staff;

Results are robust in terms of uncertainties and sensitivities to the key modeling parameters;

Key performance elements for the application have been appropriately classified and performance is backed up by

commitments.

IV.4.4 Analysis of Model Uncertainties

An appropriate consideration of uncertainties is provided in support of the proposed application. The licensee showed that the uncertainty in the risk change was small compared to the margin between the estimated change and the allowable change. This argument was supported either by explicit propagation or by a qualitative and/or sensitivity analysis showing that no event contributing to the change in risk is subject to significant uncertainty.

IV.5 Implementation and Monitoring Processes

The implementation process is commensurate with the certainty associated with the results of the deterministic and probabilistic engineering evaluations.

A monitoring program which could adequately track the performance of equipment covered by the proposed licensing changes was established. It was demonstrated that the procedures and evaluation methods will provide reasonable assurance that performance degradation will be detected and that the correction action plan will assure that appropriate actions can be taken before SSC functionality is compromised. It was also established that sufficient data will be obtained as part of the program to provide a statistically significant data base, and that data from other similar plants will be used if needed.

IV.6 Integrated Decision Making

IV.6.1 Acceptable Numerical Risk Impact

The application is either risk neutral or results in a decrease in plant risk, **OR**

If an application results in an increase in risk, the increase is within the criteria defined in Appendix B of Reg Guide DG-1061.

IV.6.2 Maintenance of Defense in Depth

The licensee has explicitly characterized the standing of the plant with respect to the criteria provided in section II.6.2, and that the proposed changes will not effect this criteria unless compensating measures are taken or unless justification is provided that the probability of failure of the non-conforming cutsets can be kept especially low.

IV.6.3 Maintenance of Risk Balance

As a result of the proposed changes, imbalances in importance are not introduced into the risk profile, or existing imbalances exacerbated, without either a net safety benefit or a convincing argument that the changes are acceptably small.

IV.6.4 Cumulative and Sypergistic Effects from all Applications

The cumulative changes in risk and in risk importance are consistent with the guidelines established in section II.6.4.

Synergistic effects have been satisfactorily addressed at the component level either

1) by assuring that multiple synergistic relaxatio' s are not applied to a single component, or

2) by noting exceptions to this, and convincingly justifying them case by case.

Synergistic effects have been satisfactorily addressed at the cutset level by showing that the modeling of compensating events is adequate, including consideration of relaxations that may have applied to them in other applications.

IV.6.5 Integration of Deterministic and Probabilistic Considerations

The process to integrate deterministic and probabilistic considerations is well-defined, systematic, and scrutable;

The Expert Panel members have the appropriate qualifications;

The Expert Panel was advised of all the specific changes and relevant background information associated with the licensing action and the panel deliberated and approved each of the changes;

The rationale for the results are auditable;

The results are shown to be robust.

V. IMPLEMENTATION

The following is intended to provide guidance to applicants and licensees regarding the NRC staff's plans for using this SRP section.

Except in those cases in which the applicant or licensee proposes a acceptable alternative method for complying with specified portions of the Commission's regulations, the method described herein will be used by the staff in its evaluation of conformance with Commission regulations.

VI. REFERENCES

1. "Status Update of the Agency-Wide Implementation Plan for Probabilistic Risk Assessment", U.S. Nuclear Regulatory Commission, SECY-95-279, March 30, 1995

2. NRC Policy Statement on "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities", (60 Federal Register (FR) 42622, August 16, 1995.

3. "Framework for Applying Probabilistic Risk Analysis in Reactor Regulation", U.S. Nuclear Regulatory Commission, SECY-95-280, November 27, 1995.

4. "PSA Applications Guide", Electric Power Research Institute, EPRI-TR-105396, August 1995.

5. Draft predecisional Regulatory Guide on Risk-Informed Decision Making, DG-1061, September 26, 1996.

6. "Standards for an Acceptable Probabilistic Risk Assessment", Draft NUREG-1602, September 26, 1996

7. "AEOD Reactor Risk Assessment Section Management Plan", S. Mays, December 15, 1995.

8. "Procedures for Treating Common Cause Failures in Safety and Reliability Studies", NUREG/CR-4780, January 1988

9. "Severe Accident Risks: An Assessment for Five Nuclear Power Plants," NUREG-1150, Volumes 1 and 2, December 1990

10. "Common-Cause Failure Data llection and Analysis System", Draft Volumes 1 through 6, INEL-94/0064, December 1995

Appendix A Miscellaneous Probabilistic Evaluation Issues

A.1 Use of Plant Specific Data

a. Area of Review:

In selecting appropriate failure rate data to use in the risk-informed applications, the analyst is frequently faced with the question of whether to use plant specific or generic data, or some combination of the two. For newer plants with little operating history, the only choice is use of generic data, in which case the only decision is which generic data base to use. For those cases where significant plant specific data are available, usually it is most appropriate to combine plant specific and generic data with a method that gives appropriate weight to each. The Bayesian updating method is usually employed in these cases. Since several generic data bases are available, and they do not always agree, a further issue is which of these is most appropriate.

As the proposed application is phased in, revisiting failure data becomes more important. It also becomes more important for each licensee to review operating experience (in particular, degradation mechanisms) experienced at other plants for applicability to the licensee's plant. Performance monitoring at individual plants cannot be expected to provide sufficient experience to statistically justify failure rates significantly less than generic failure rates without reference to the operating experience of other plants.

Finally, in considering plant-specific failure data, it is important to be able to recognize poorly-performing individual components, rather than allowing poor performance of a single component to be averaged over all components of that type. Relaxing requirements based on a failure rate derived by averaging over a large number of components including one poor performer could lead to a significant probability of experiencing an in-service failure.

b. Description of the Methods Acceptable to the Staff for Addressing this Issue

For those cases where statistically significant plant specific data are available, it is acceptable to use such data if they are appropriately combined with generic data. The Bayesian updating approach is an acceptable method to use, provided that the prior distribution (generic data) represents the characteristics of the component and the evidence (e.g., statistical data) is compiled and used correctly. The Bayesian updating approach then gives appropriate weight to both generic and plant specific data. For those licensees who propose to use plant specific data only, the data used must either be consistent with that employed in NUREG-1150 (or in the AEOD databases for CCFs and initiating event frequencies), or any significant deviations must be justified. Significant in this context can be defined as no greater than a factor of 3 for the mean values of the failure rate. For those licensees who propose to use only generic data, or to combine plant specific data with generic data, the generic data base used should also be consistent with that used in NUREG-1150.

When the PRA is updated periodically, components that have experienced failures should be checked for evidence that they are especially poor performers. An extreme example of such evidence would be multiple failures experienced by a single component in a class whose other members have experienced no failures over the same interval. Components that have experienced failures should be reviewed to see whether plant commitments would be considered adequate to support the performance expected of them, based on a component-specific failure rate consistent with the number of failures experienced.

c. Acceptance Guidelines

The acceptance guidelines for this issue are as follows:

The generic failure rate data used in the risk-informed program should be consistent with that used in the AEOD databases or in NUREG-1150 unless the licensee can provide a basis for using generic data which is different.

The plant specific data, if employed, should also be consistent with NUREG-1150 unless it can be clearly shown, with statistically meaningful methods, that the plant specific data are more valid.

The process must consider the possibility of poorly-performing individual components, and check for indications of this by reviewing plant operational experience data when the PRA is updated.

d. Review Procedure

The review procedure consists of the following steps:

1. The SSC failure rates are compared with the values given in NUREG-1150 to see if they are consistent (within a factor of 3).

2. If the failure rates are not consistent with the NUREG-1150 values, a review is made of the basis for the values used to assure that the deviations from NUREG-1150 are justified. If the deviations are due to plant specific data, a review is undertaken of the statistical significance of the plant specific data, and possible reasons for the differences. If the deviations are due to generic data, they are not accepted unless justification is provided. This justification includes the data sources used as input for the generic data, as well as the statistical models employed to derive the failure rates.

3. The reviewer looks for evidence that the Expert Panel specifically reviews components experiencing failures in the plant, in order to assess whether individual components are performing significantly more poorly than the average performance of the population of which they are members. For example, the Expert Panel should have documented application- specific components that have suffered from two or more failures and have considered this history in the panel deliberations.

e. Evaluation Findings:

The reviewer verifies that information was provided to support the following conclusions:

The failure rates used, especially those that directly affect the proposed application, appropriately consider both plant specific and generic data that are consistent with AEOD data or with NUREG-1150, or the deviations are justified.

Credit for especially low failure rates (i.e., relative to generic failure rates) is supported by an appropriate performance monitoring program, and by review of other plants' operating experience.

The licensee systematically considered the possibility that individual components could be performing more poorly than the average associated with their class, and avoided relaxation for those components to the point where the unavailability of the poor performers would be appreciably worse than their performance targets.

A.2 Truncation Limits Used

a. Area of Review

As a result of computer model and time limitations, the quantification process to evaluate CDF or LERF would involve cutset truncation either by use of a cutoff frequency or a maximum cutset order. Since the truncation process eliminates accident sequences from further consideration, care has to be taken to ensure that important sequences are not discarded and that the final results are not sensitive to the truncation limit chosen.

b. Description of the Method(s) Acceptable to the Staff for Addressing This Issue

The selection of truncation values for the quantification of accident sequence frequencies is discussed in NUREG-1602. Acceptability of a truncation value used in the baseline PRA should be reviewed as part of the "quality" of the PRA (in the licensee peer review process). On an application specific basis, licensees should also demonstrate that the effects of the application on components modeled in the PRA is not restricted by the truncation criteria chosen. This could include sensitivity studies using different truncation levels (to selected parts of the model), or by the requantification of the base model from the beginning (as opposed to use of a pre-solved model) when evaluating the risk for the proposed applications.

c. Acceptance Criteria

The general rule is that the truncation criteria has to be low enough so that there is evidence of convergence towards a stable result.

For all applications the licensee has to show either quantitatively by use of sensitivity studies or qualitatively by use of engineering arguments, that the truncation limit chosen will not affect the calculation of risk contribution from SSCs for which a change in regulation is proposed i.e., the licensee should verify that the inputs supplied to the Expert Panel, and the panel's conclusions are not adversely affected by truncation.

d. Review Procedures

The reviewer should be assured (either by documentation provided in the licensee peer review or by a staff review) that cutset truncation has not introduced errors into the results or the logic of the PRA. Staff review could also involve the performance of (or the review of) sensitivity studies where the truncation limit is lowered for the dominant sequences and event initiators, and a study of the resultant cutsets to see if there are any hidden dependencies or unusual/unexpected event combinations especially if these involve components affected by the proposed application.

In PRA models where common cause failures and human dependencies are incorporated at the sequence level after a truncated set of minimal cutsets has been obtained, the reviewer should check that the truncation criteria used in the PRA do not lead to cutsets involving application specific components being truncated that could be important if common cause failures, dependencies and uncertainties are considered.

Staff review could also include a comparison of a list of all the events affected by the application that is in the final truncated CDF cutset equations to the list of basic events used in all fault tree and event tree models. This will yield a list of events that did not make it past the truncation process. Documentation should be available as to why each of the truncated events is not important to the CDF risk. [Alternately, the minimal cutsets can be re-generated with unavailabilities set to a high value (e.g., 0.5) for those elements affected by the application. This will ensure that truncation effects on the application specific elements is small.]

Finally, the reviewer should ensure that the evaluation of the change in risk from the application was performed by the requantification of the base model at the fault tree /event tree level so that the potential effects of originally truncated events could be accounted for should they become important as a result of the application.

e. Evaluation Findings

The staff review should conclude that the licensee has satisfactorily established that the inputs supplied to the Expert Panel, and the panel's conclusions are not adversely affected by truncation i.e.,

the truncation criteria is sufficiently low to obtain stable results, i.e., the magnitude of the CDF or release frequency will not change as a result of lower truncation limits, and the grouping of SSCs into risk categories will also not be affected.

the components affected by the application are, for the most part, not truncated out of the model. In cases where they are, a qualitative assessment (using perhaps a Expert Panel process) can demonstrate the reasons why they are unimportant to the risk.

A.3 Determination of Success Criteria

a. Area of Review:

Guidance in the PRA policy statement stipulates that best-estimate analysis should be used in PRA implementation. The following discussion is aimed at sorting out what is meant by "best-estimate" analysis of success criteria by reference to SAR analysis.

In order to fulfill its intended purpose, SAR analysis is ordinarily based on a set of assumptions containing significant embedded conservatisms. SAR analysis also reflects a postulated single active failure in addition to whatever event initiated the sequence. When a SAR analysis shows a successful outcome, then, there is good reason to believe that apart from beyond-single-failure scenarios, the system will meet or exceed performance requirements, at least for the initiating event considered.

Applying the SAR mission success criterion in a PRA would clearly be conservative, in the sense that the probability of failure to meet this standard of performance would be significantly greater than probability of failure to meet a more realistic standard of performance, such as preventing severe core damage while taking credit for potential success of beyond-single-failure configurations of the system. However, re-analyzing event sequences with conventional SAR tools would be too expensive to apply to the large number of scenarios that are defined in the course of a PRA, and in fact the rather specialized computer codes used in SAR analysis would, in many cases, not work properly in beyond-single-failure scenarios, which are beyond the intended domain of those codes' applicability. Traditionally, then, development of mission success analysis in PRA has ranged from simulation of a large number of scenarios using fast-running models that would not be considered fully quality-assured but that are at least not systematically conservative, down to simulation of a few cases and extrapolation of results to other cases by an Expert Panel, or perhaps extrapolation from analysis performed on similar plants.

For success criteria calculations to be acceptable as a basis for risk-informed allocation of safety resources away from particular items, the types and quality of calculations and computer codes used must meet standards as specified in (c) below. In addition, it has to be recognized that equipment configurations deemed "success" may have an appreciable probability of actually corresponding to functional failure, i.e., the nominal minimally successful equipment configuration might not, in fact, yield successful performance 100% of the time. In the area of risk-informed regulation, this possibility must be considered carefully.

In order to satisfy the Commission guideline, then, the staff must find that the applicable PRA insights have not been distorted by a systematic conservative bias in mission success criteria, and that mission success criteria used to justify relaxation of regulatory requirements have a rigorous technical basis, even if they are not based on the same computer

codes as those used in SAR analysis.

b. Description of the Method(s) Acceptable to the Staff for Addressing This Issue

In principle, the staff may consider independent analysis of each mission success criterion. However, this will be warranted only in cases where the results are especially sensitive to the particular assumption, and/or the modeling is particularly controversial.

Staff reviewers should recognize that some mission success criteria are testable, and in fact may even correspond to configurations that arise in normal plant operation. Some configurations are not normally encountered, and in some cases, entering a "success" configuration would impose burdens of various kinds. Bleed and feed cooling is an example of the latter. Remoteness of a given configuration from normal experience can be considered by the staff in its assessment of the adequacy of the technical basis for a particular mission success criterion.

While the reviewer must always be alert to the possibility that plant-specific features may invalidate a comparison of criteria from one plant to another, it is to be expected that some mission success criteria can validly be extrapolated between similar plants. This is meaningful only when a firm basis for the criterion is created at the first plant; it is not the intention of present guidance to sanction widespread acceptance of a mere assumption in the name of "consistency."

c. Acceptance Guidelines:

The models, codes, and input must meet QA standards that are consistent with general accepted methods, and the models, codes and input should have been reviewed by the independent peer review group as well as the Expert Panel as appropriate for specific applications. The QA standard should include configuration control of the analysis input and results. The standard does not have to be the same as the standard applicable to SAR analysis, but it must be explicit (i.e., engineering calculations and codes must be verified and quality assured) and it should be formalized by the licensee as part of the licensee QA program.

AND

The analysis must demonstrate that the configuration is successful with sufficient margin that the probability of "failure" in the nominally successful configuration is negligible compared to the probability of failing to achieve a successful configuration

OR

The analysis must quantify the probability of "failure" in the nominally successful configuration. Either the licensee must make this representation on the record, or the staff reviewer must establish it independently.

d. Review Procedures:

As part of the review of the general "quality" of the PRA, the reviewer should verify at a minimum that the licensee has indicated all success criteria invoked in the analysis, and the basis for each. Note that every success path on every event tree is based on a mission success criterion, and that in principle, a large number of these may be distinct. For a given success path, if the basis for the mission success criterion is analytical, then code version and input data should be specified, or at least maintained on file for possible inspection. In the case of a PRA formulation that generates many distinct success criteria, the licensee should represent that a complete set has been specified.

If the analytical basis makes essential use of computer codes that have not received substantial review, then closer examination of the mission success criteria may be appropriate. If a closely similar plant has used similar criteria, with substantial justification, these criteria may be used as a reference point. If the results are sensitive to the criterion, and their basis is lacking, then the reviewer must either ask for additional justification or seek independent analysis.

On an application specific basis, the emphasis of the review should be on whether the definition of the system success criteria will be affected by the application specific elements or the elements required in the same minimal cutset as the application specific element. The licensee and reviewer must assure that the success criteria is not optimistic so as to underestimate the number of components required (i.e., overestimate the size of the minimal cutset).

The reviewer should verify that essential mission success criteria that are submitted by the licensee to justify relaxations are understood by the licensee to be part of the licensing basis thereafter.

e. Evaluation Findings:

The staff safety evaluation report should contain findings equivalent to the following:

A technical basis has been established for each mission success criterion used in the analysis. Analytical elements of the technical basis have been configuration-controlled and quality-assured. Experimental (operational) demonstrations of the success of particular system alignments are cited. Where comparison with analogous criteria from other plants is possible, this comparison has been presented.

The probability that "successful" configurations actually correspond to functional failure is either explicitly quantified, argued convincingly to be negligible compared to the probability of being in a nominally unsuccessful configuration, or shown to be irrelevant to the application.

A.4 Modeling of Common Cause Failures

a. Area of Review

Common cause failures (component hardware failure dependencies) cover the failures of usually identical components that are usually caused by design, manufacturing, installation, calibration or operational deficiencies. Because they can fail more than one component at the same time, CCFs can dominate plant risk.

Risk-informed applications that cover SSCs as a group have the potential of being affected by the CCF probabilities. For the affected components, CCF probabilities could be low or might not even be included in the baseline PRA models based on the historical and engineering evidence driven by current requirements. With proposed changes there must be assurance that the CCF contribution will not become more significant.

b. Description of the Method(s) Acceptable to the Staff for Addressing This Issue

The licensee should document that potentially significant CCFs have been covered in the PRA and that the effects of the proposed changes have been incorporated into the CCF modeling. This documentation should include a discussion of the process used for the selection of common cause component groups.

Acceptable methods for the derivation of CCF probabilities are presented in NUREG-1602 which recommends the methods and database from the AEOD report "Common Cause Failure Data Collection and Analysis System". For cases where the

database needs to be expanded to include numbers of components beyond that addressed in the AEOD report (generally six components), it should be assumed that the conditional probability of each subsequent component is the same value as was in the sixth component in the AEOD database. Using lower generic common cause values than those shown in the AEOD report or eliminating a common cause treated in the AEOD report are discouraged and are generally deemed inappropriate. However, specific cases will be considered if ample justification is provided by the licensee.

On an application specific basis, licensees should model CCF of groups of similar components that are being affected by the application if there is a basis for the potential likelihood of CCFs based on operational considerations and historical data. Licensees should have identified such groups, and established that performance monitoring is capable of detecting CCF before multiple failures are allowed to occur subsequent to an actual system challenge.

c. Acceptance Criteria

CCF modeling of failures potentially addressed by the application must be performed. This includes the modeling of CCF groups of similar SSCs that are mutually redundant and all being relaxed.

To reduce fault exposure times for potential common cause failures (especially in cases where risk impact is relatively large compared to the allowed risk increase), phased or incremental implementation should be considered as part of the effort to protect against CCF.

d. Review Procedures

The reviewer should check to confirm that potential CCFs which involve components affected by the application have been considered in the PRA. It is particularly critical that the selection of common component groups was performed correctly to ensure that important common cause failure groups were not omitted.

The reviewer should verify that industry and especially plant specific experience which involve the failure of two or more components (especially for the application specific components) from the same cause was analyzed and incorporated into the model where appropriate. In this case, "failures" should include multiple corrective maintenance actions for the same cause on multiple components.

The reviewer should determine that the methodology used to calculate the CCF probabilities is consistent with that given in the AEOD report (reference 10). Consistency of common cause failure probabilities with past experience and with the AEOD data should also be checked.

For all applications, reviewers should check that licensees have appropriately modeled CCF of groups of equipment that were proposed for the change, and have established that performance monitoring is capable of detecting CCF before multiple failures are allowed to occur subsequent to an actual system challenge.

e. Evaluation Findings

Evaluation findings should include statements of the following effect:

Common cause failure has been suitably addressed and that the licensee has systematically identified all component groups sharing attributes that correlate with CCF potential and that affect the application.

The licensee's performance monitoring program addresses a phased implementation approach to reduce the potential for common cause failures.

A.5 Modeling of Human Reliability

a. Area of Review

The results of a PRA, and therefore the decisions that are informed by it, can be very strongly influenced by modeling of human reliability. Plant safety depends significantly on human performance, so it is essential that PRAs treat it carefully. However, the modeling of human performance is a relatively difficult area; significant variations in approach continue to be encountered, and these can significantly influence the results. In addition to the variability issue, there are policy questions related to what kind of human actions can appropriately be credited in the context of a particular regulatory finding. As an example, suppose that PRA results appear to support relaxation of requirements for a component based on the argument that even if the component fails, its failure can be recovered with high probability by operator actions outside the control room. The issues of concern here are whether the modeling of the operator action and the evaluation of the failure probability is appropriate, and whether this kind of credit is the sort of compensating measure that is intended by staff guidance to support justification of a relaxation.

b. Description of the Method(s) Acceptable to the Staff for Addressing This Issue

NUREG-1602 describes acceptable methods for quantifying human performance. For purposes of many risk-informed applications, the issues are narrower in that they are related not to the methods of quantification but rather to the allocation of performance credit between plant operators and plant equipment. Licensees should indicate all human actions that compensate for events affected by the proposed application, and show that inappropriate credit has not been taken for these events.

c. Acceptance Guidelines:

For purposes of evaluating a plant's defense in depth attributes, recovery of failed equipment should not count as a barrier. Human actions to actuate equipment as part of the normal, proceduralized accident response may be counted as if the human action were an active component function (e.g., manual switchover to ECCS recirculation following a LOCA in a PWR). Recovery of selected functions may be counted along lines spelled out in NUREG-1602, which promulgates acceptable probability values for selected events. Licensees that take this kind of credit must explicitly commit programmatic resources to it (training, etc.).

Justification of relaxations in current regulations should not be based on credit for post-accident recovery of failed components (repair or ad hoc manual actions, such as manually forcing stuck valves to open). Credit may be taken for proceduralized implementation of alternative success strategies to work around a failed component.

For each human action that compensates for a basic event probability increasing as a result of relaxation in a regulation, there should be an explicit licensee commitment to ensure performance of the function at the level credited in the quantification. Excessively low human failure probabilities (less than 0.001) cannot be accepted unless an appropriate commitment can be shown in the plant's training programs, personnel practices, staff policies, and staff performance.

d. Review Procedures

The comprehensive review of human reliability modeling should be treated as part of the peer review of the baseline PRA. Staff review should focus on a review of the peer review documentation. In addition, the review should also consider

application specific events, specifically, the quantification of compensating human actions. The reviewer should confirm that credit for compensating human actions is limited to proceduralized actions taken to actuate systems; repair of failed equipment should not to be considered. The intent of this review element is to ensure that licensees do not relax regulations on the basis of arguably speculative and relatively uncertain quantification of recovery probabilities.

e. Evaluation Findings:

The staff safety evaluation report shall include language that is equivalent in effect to the following.

The modeling of human performance is appropriate.

A systematic approach is taken for the identification of errors of omission; the probability values used for these errors reflect plant procedures, plant instrumentation, and plant staffing practices. Quantification of these error probabilities is based on up-to-date approaches to quantification.

An attempt has been made to identify credible and risk-significant errors of commission potentially resulting from the application, and to quantify their probabilities.

Appropriate credit is taken for the ability of the human to help the plant respond. Proceduralized actions to ensure actuation of appropriate systems are addressed, and failure to perform these actions is addressed if it is significant. Proceduralized actions to control systems are addressed, and failure of proper control is addressed if it is significant.

Post-accident recovery of failed components is modeled in a defensible way. Recovery probabilities are not quantified in a clearly non-conservative way. The formulation of the model shows decision-makers the degree to which the apparently low risk significance of certain items is based on credit for recovery of failed components (restoration of component function, as opposed to actuation of a compensating system).

The licensee recognizes the importance of, and is committed to ensuring, human performance in those situations in which the PRA has shown it to be particularly significant.

A.6 Requirements for a Living PRA

a. Area of Review

This issue encompasses the need for maintaining and updating the PRA used for the risk-informed program, as well as requirements to assure that the maintenance and updating is comprehensive, appropriate, and timely. Changes in programmatic activities need to be reflected in the PRA so that future decisions regarding modifications to programmatic activities are not based on obsolete information.

In addition to this concern, PRA technology continues to be an evolving field, and methodology improvements are likely to occur in the future. Further, as the current population of nuclear plants continue to mature, more comprehensive data on component failure rates, human error consideretions, initiating events and dependencies will accrue. It is important that this information be periodically reviewed and incorporated, as appropriate, into individual licensees' PRAs to assure that risk-informed decisions continue to be supported. As the PRAs are improved by the inclusion of this information, they should be periodically used to recompute the metrics used in the risk-informed decisions to assure that the conclusions remain valid.

b. Description of the Methods Acceptable to the Staff for Addressing this Issue

The licensee is required to reflect plant modifications in an updated PRA on a regular basis. In addition, the licensee should commit to a program which assures that appropriate information developed from PRA activities in the rest of the industry are incorporated into the PRA on a timely basis. The sources for such information include research activities sponsored by EPRI, INPO, NEI, NRC, DOE, and IAEA, as well as information from the licensees own plant as operating experience is gained. Further, updating which is done by other licensees to their PRAs should be monitored to identify appropriate changes to the PRA. Foreign research activities should also be monitored and included in the updating, as appropriate. The updating should be done every refueling outage, or every two years, whichever is more frequent, unless it can be shown that no new relevant or significant PRA information has been developed during the time interval. The licensee should also commit to a program of verifying the PRA after each updating process. This verification is performed to assure that the input for the updating has been correctly programmed into the PRA, and that the PRA logic remains sound. If the updating affects in any way the models used for risk-informed applications or supporting data, then the PRA must be used to confirm that the low risk significant components remain low, and that the risk change resulting from the applications is not significantly different than that from the original analysis.

c. Acceptance Guidelines:

The acceptance guidelines for PRA updating requirements is as follows:

The licensees risk-informed program must include provisions for updating the PRA every refueling outage, or every two years, whichever is more frequent, unless it can be shown that no new relevant PRA information has been developed during the time interval.

The updating process must include verification of the PRA after updating information has been programmed into the PRA.

If the updating information has a substantial influence on the models or data, then the PRA must be used to re-establish the risk change for the affected risk-informed programs.

d. Review Procedures:

The review procedures involve the following steps:

The licensee's risk-informed program proposal is reviewed to assure that provisions exist for updating the PRA.

The sources of information that are to be used to update the PRA are reviewed to assure that all relevant sources are included, see (b) above.

The PRA updating program is reviewed to assure that PRA validation procedures following each major updating are included.

The program is reviewed to determine the proposed frequency of the updating activity. This frequency should conform with the provisions in (b) above, or justification provided for a different schedule.

If the information used for the updating is expected to have an influence on the estimated risk change for the risk-informed program, then a recalculation of the risk change must be included to assure that the risk-informed program still meets the original criteria.

e. Evaluation Findings:

The reviewer verifies that the information provided and review activities support the following conclusions:

The PRA used for the licensees proposed risk-informed program includes a provision for periodically updating the PRA at a suitable frequency.

The updating procedure includes screening of all relevant sources for providing information appropriate for updating the PRA.

The updating procedure includes provisions for validating the PRA after each updating.

The procedure includes a provision for recalculating the change in risk for all the proposed and previously implemented risk-informed programs if the updating information affects the modeling of the components affected by the application.

Appendix B Expert Panel Issues

B.1 Use of an Expert Panel

a. Area of Review:

In general, it is a requirement in RIR applications that a responsible panel of experts oversee each PRA application. This is true for many reasons. It is desirable to vest the responsibility for such important findings in a recognized and organizationally stable entity. Applying the PRA and integrating PRA results with other analyses to formulate defensible conclusions requires an inter-disciplinary perspective that can be provided by an Expert Panel. Also, the performance of the PRA will not in general have anticipated any given focussed application, so there is a need for an inter-disciplinary check of whether, in a specific application, the PRA analysis is being utilized beyond its domain of applicability. There is also the need to address the imperfections and shortcomings that are inevitable in any model of a facility as complex as an NPP. Finally, there may be a need to extrapolate PRA insights to areas that have not been explicitly analyzed using PRA. These reasons are in addition to the analytical role played by the Expert Panel, which in most cases will be the decision-making body that actually applies PRA and deterministic results to justify the acceptability of proposed applications.

However, although the Expert Panels can be held accountable for a great deal, there is a limit to how far they can legitimately go without a suitable PRA foundation. The present question is what kind of shortcomings can be accepted in the PRA for risk-informed applications, and how severe can they be, without placing excessive demands on the Expert Panel process.

b. Description of the Method(s) Acceptable to the Staff for Addressing This Issue

Generally, it must be shown that the information base supplied to the Expert Panel is capable of supporting the findings that must be made in the context of the specific risk-informed application.

1. Before the Expert Panel takes up an application, there must be an inventory of plant response capability for each operating mode and each initiating event category (internal, external, flood, fire, seismic, etc.). Given a fully-scoped level 2 PRA, this requirement could be satisfied by an inventory of event tree success paths, with an indication of the mission success criteria, systems, and SSCs involved in each path. Lacking a fully-scoped level 2 PRA, surrogate information must be developed for unanalyzed areas, along the lines described under the issue "Scope of the PRA". It is expected that licensees already have compilations of much of this information, essentially to support other (licensing) program areas. For example, the current licensing basis should contain much of this, although perhaps formulated on the basis of conservative mission success criteria.

   This requirement is necessary in order to show what safety function is performed by SSCs affected by the application.

2. Causal models (determination of cause-effect relationships) must be developed to support quantification of basic event probability as a function of the application and other programmatic activities.

   This is necessary in order to relate the application to actual risk indices, and to calculate importance measures.

3. At least the level 1 portion of the internal events PRA must be formulated in such a way as to support quantification of importance measures (CDF and LERF), and must provide qualitative (minimal cutset) information adequate to support defense in depth findings.

While it is possible to accept program reductions for components that are explicitly shown to play no role in unanalyzed operational modes, it is much more difficult to accept reductions for components that do play a role in unanalyzed (e.g., shutdown) modes. For such instances, conservative methods will be considered prudent.

c. Acceptance Guidelines:

The conditions as specified in (b) above should be met for all applications. In order for an application to proceed, the scope of it must match the information base along lines indicated in (b). That is, shutdown information must exist in order to support findings about SSCs playing a role at shutdown, etc. Note that if no information is provided about shutdown, then it will be difficult to justify changes in policy, because in a formal sense, there are no grounds for concluding that a component is not needed at shutdown.

d. Review Procedures:

Documentation of inputs to the Expert Panel is required as part of the process. The Expert Panel affirms the adequacy of this information base. The reviewer should, however, verify the scope and depth of the information base, especially the character of information supplied regarding modes and/or classes of initiators unanalyzed in the PRA.

e. Evaluation Findings:

The following language, or language substantially equivalent to this, should appear in the SER, or else exceptions should be noted and explained.

The Expert Panel was provided with a technical information basis that was adequate for the scope of the application that was actually performed. In particular, the analysis of success and failure scenarios was adequate to identify the roles played by the SSCs affected by the application, the quantification of the frequency of these scenarios was adequate to establish the safety significance of the SSCs, and the causal models were adequate to establish the effects of the proposed changes in the program.

B.2 Expert Panel Process

a. Area of Review:

The role of the Expert Panel in RIR is critical. However, it is not practical to externally validate all Expert Panel deliberations, because of the nature of the integrating role played by the Expert Panel, and the volume and diversity of the information that is involved in its deliberations.

Assurance of the appropriateness of Expert Panel decisions must therefore be derived through means other than replication of its work. One such means is consideration of the character of its process, including its documentation of its deliberations and findings.

b. Description of the Method(s) Acceptable to the Staff for Addressing This Issue

The members of the Expert Panel should include personnel with considerable experience in engineering, risk analysis, plant operations, maintenance, safety analysis, and personnel familiar with the particular application (e.g., IST engineer, a maintenance engineer, a QA specialist, etc.). Each member should have a minimum of 5 years' experience at the plant being considered in the risk-based program, or at a similar plant. Each member should have recognized competence in his or her area of expertise.

Because of the significance of the Expert Panel's deliberations, and the level of trust that is placed in the Expert Panel, it is required that the panel proceed in a relatively formal way, and document its activities in a relatively formal fashion. The staff may not routinely audit all of the Expert Panel's findings or recommendations, but the documentation must exist to support such a review, and must be maintained until such time as the recommendations are invalidated by later changes to the plant or to the analysis. That is, since Expert Panel findings may effectively enter the licensing basis, they must be maintained until invalidated.

It is expected that a part of the Expert Panel conclusions will be the use of compensatory measures as a part of the proposed application. For these cases, it is important that the Expert Panel clearly document why the compensatory measures are an appropriate substitute for a proposed relaxation in current regulations, and that the compensatory measure becomes part of a plant commitment.

In performing the evaluations and determinations for a risk-informed application, the Expert Panel should consider information from the risk analysis, deterministic insights, quantitative sensitivity studies, operational experience, engineering judgment, and current regulatory requirements. However, final determinations will have to be consistent with criteria as provided in section II.6.

c. **Acceptance Guidelines:**

Most risk-informed applications must include the use of an Expert Panel to integrate probabilistic and deterministic analyses. This panel must include members with recognized expertise and experience as indicated in (b) above. The panel would review every SSC that is proposed for program relaxation, independent of the initial risk significance determination. The panel should provide comprehensive documentation of their deliberations and decisions, and this documentation should be archived for future retrieval and review.

While replication of the Expert Panel's work will not normally be performed, the standard required of documentation is that it be capable of supporting such a replication in detail. The justification for this high standard is the great significance of the work of the Expert Panel, and the fact that many of its decisions may affect the licensing basis.

d. **Review Procedures:**

Technical issues are discussed under other sub sections. If substantial technical problems emerge as a result of review of other areas, then this reflects on the process, and should be considered in the review of the process. However, the focus of the present section is the process itself.

Because the focus of this item is on process, the only way the staff has to review this area (short of being present for Expert Panel meetings) is Expert Panel documentation. Accordingly, the reviewer must examine documentation of:

Expert Panel organization and membership;

Information base made available to panel (e.g., PRA, system notebooks, PRA importance rankings, etc.); and

Records of deliberations (issues raised, decisions made, findings/ recommendations, requests for analysis, determinations of risk contributions from SSCs, basis for decisions/findings/recommendations).

e. **Evaluation Findings:**

The following language, or language substantially equivalent to this, should appear in the SER, or else exceptions should be

noted and explained.

An Expert Panel was formed and utilized in the development of the risk-informed program.

The Expert Panel membership met the requirements for competence in a pertinent discipline, experience, and training.

The Expert Panel process is appropriate. The process ensured that information required was collected, that suitable issues were raised, that the process of disposition of those issues was systematic and defensible, and that the documentation of the deliberations is traceable and reviewable in principle, so that the basis for findings and recommendations is available for scrutiny and review. Compensatory measures invoked by the Expert Panel to justify relaxation of requirements are captured as commitments.

The Expert Panel's final evaluation of risk significance represents appropriate consideration of probabilistic information, deterministic evaluations, sensitivity studies, operational experience, engineering judgment, and current regulatory requirements.

B.3 Use of Expert Panel to Overcome Potential Limitations of the PRA Model

a. Area of Review:

Separate sections of this SRP have addressed SSCs not modeled in PRA, scope limitations, and use of system importance to overcome single-event importance. This section focusses primarily on modeling inadequacy in those portions of the PRA that actually exist.

Part of the Expert Panel's job is to overcome certain limitations of the PRA; however, this does not include substituting the panel's judgment for essential PRA results. One of the reasons for developing PRA models in the first place is that the complexity of many facilities makes judgment unreliable in many contexts.

Generally, if PRA highlights a vulnerability in some area, this should be taken seriously. The result should not be discounted on the basis of judgment; if the Expert Panel can show that the PRA representation of a vulnerability is invalid, then the PRA should be modified, subject to the procedures governing substantial PRA modifications, and the panel should work with the results of the revised PRA.

However, it is expected that important issues may go unrecognized in straight-forward PRA analysis and in the analysis of component risk importance. There are several reasons for this. One reason is that conventional importance analysis is not a totally reliable indicator of insignificance: items that appear insignificant in importance analysis are not necessarily insignificant, even if the model is not defective. Another reason is the possibility of modeling choices that neglect or obscure an important issue. This is not necessarily a PRA shortcoming. It may arise in an application because the PRA was not performed with the application in mind; in such a case, its baseline quantification may be essentially accurate, but the model might not have allowed for analysis of sensitivities to changes in that application. It is the job of the Expert Panel to identify such issues.

For applications at plants whose PRAs do not address all modes or all classes of initiating events, the Expert Panel has an extremely important job. For example, in a plant whose PRA only addresses full power, the Expert Panel must make findings about SSCs that potentially affect shutdown as well. This must be done by the Expert Panel using the non-PRA information about shutdown that is itemized in other sections of this SRP, based on the role that those components play in plant response at shutdown and at full power.

b. Description of the Method(s) Acceptable to the Staff for Addressing This Issue

To address the issue of credit for unmodeled systems that would change a PRA result, the acceptable method is to alter the PRA to take the credit. This modification should be treated under the protocols that govern modifications to the PRA (as defined in NUREG-1602). Judgment-based credit is not a surrogate for PRA analysis. There may be cases in which the problem is simple and transparent and the conclusion can readily be drawn; in such cases, the PRA will be easy to modify. There are potentially cases in which credit for an unmodeled system would be seriously complicated by issues of shared support systems, environmental conditions, or other factors that the discipline of the PRA process is intended to discover. These instances are the reason for insisting on a formal treatment.

To address the issue of making decisions about SSCs that might influence plant response in unmodeled modes or to unmodeled initiators, the acceptable approach is to proceed on the basis of a structured representation of plant response that shows at least qualitatively what initiating events pertain, what systems are available to respond to each, functional dependencies of these systems at the train level, and in particular, what backups are available in the event of failure of any particular component.

Since these decisions effectively enter the licensing basis, they should be made with the formality described under Expert Panel process, and documented accordingly.

To address instances in which a PRA model exists but is considered misleading, caution is indicated. The above guidance suggests that it is basically unacceptable to place on the record both a PRA and a finding that clearly contradicts it. On the other hand, the Expert Panel is not required to take the PRA as absolute truth. The test should be whether the record establishes a clear basis for a finding. A technical argument that begins with the misleading PRA result and furnishes supplementary information sufficient to justify a relatively minor change to a PRA result, or a qualified interpretation of a PRA result, is satisfactory. A cursory technical argument leading to a conclusion that qualitatively contradicts a major PRA result is an unsatisfactory record.

c. Acceptance Guidelines:

The Expert Panel should not enter judgments based on credit for features not modeled in the PRA. In particular, if a vulnerability seems overstated in the PRA as a result of failure to take credit for a system or an operator recovery action, then the PRA should be modified. The Expert Panel should not discount the vulnerability on the basis of its judgment.

However, the Expert Panel is expected to identify possible concerns that are not manifest in PRA results.

Down-classifying SSCs (i.e., stating that a high risk contributor is actually a low contributor) from a PRA result, based on Expert Panel judgment, should receive very close scrutiny. It would ordinarily be preferable to modify the PRA, subject to the appropriate protocols, and then re-perform the classification exercise. This guidance is based on the perception that the record of such a decision almost inevitably has the appearance of unreliability: the panel is contradicting the results of an integrated plant model on the record.

Other issues should be judged by how far from the established models the Expert Panel is required to go. The farther the panel must travel on its own judgment, the longer and more complex the record of decision will need to be. The overall goal of the process should be to iteratively improve upon the models, not regularly transcend them in major ways. A long, complicated record of decision is an indication that the PRA should have been modified.

d. Review Procedures:

The reviewer should check to see whether the application involves SSCs that have been shown to be potentially high risk contributors by the PRA, and if so, should scrutinize the basis used by the Expert Panel for this action.

If the Expert Panel takes exception to a PRA finding, this should be a matter of record. The reviewer should examine records of Expert Panel deliberations to identify instances in which the panel noted a limitation and overcame it. The reviewer should be aware that while PRA indications of importance generally need to be taken seriously, typical PRA results of unimportance, taken at face value are not as reliable, not necessarily because of model shortcomings, but because PRA models are not usually applied in such a way as to support valid conclusions regarding unimportance (see the discussion of sensitivity studies and other considerations required as part of the risk importance determination process in Appendix C). Therefore, if the Expert Panel finds that something is more important than the PRA importance measures seemed to indicate, this should not in itself be grounds either for doubting the panel or for doubting the PRA.

The reviewer should check for instances in which the Expert Panel took exception to a PRA result and was obliged to develop an extended argument to justify it. The need to go to an extended argument is a suggestion that the PRA should have been modified.

e. Evaluation Findings:

The following language, or language substantially equivalent to this, should appear in the SER, or else exceptions should be noted and explained.

The process applied by the Expert Panel to overcome inevitable limitations of PRA was appropriate. Where the panel felt obliged to make decisions that would not follow straight-forwardly from the PRA, the panel provided a technical basis for the decision that shows how the PRA information and the supplementary information validly combine to support the panel's finding. No panel finding contradicts the PRA in a fundamental way. Where the PRA can and should be modified in future to do a better job, the panel has indicated this on the record.

B.4 Use of Expert Panel for Treatment of SSCs not Modeled in the PRA

a. Area of Review:

It is not possible for PRAs to explicitly model all SSCs involved in performance of safety functions. Modeling all SSCs would require display of many items that are logically necessary for system function, but whose failure is not believed to dominate system failure, and whose failure in any case is not believed to link failures of different systems. If an unmodeled SSC is believed to link failures of different systems, then it arguably should have been modeled, unless there are strong grounds for believing that the failure is extremely unlikely.

These omissions are not to be considered shortcomings of PRA. The point is that PRA is usually done with a view towards quantifying the status quo, and modeling priorities and modeling shortcuts are established accordingly. In RIR, however, the PRA is used for allocation of programmatic resources over SSCs, including SSCs that are modeled explicitly, SSCs that are implicitly reflected in modeled elements, SSCs that were effectively screened out in the modeling but need consideration in RIR, and perhaps SSCs that were simply neglected. In some cases, SSCs are omitted based on analysts taking credit for programmatic activities that ensure a low failure frequency for that item or a short fault exposure time in the event that it does fail. In such cases, when PRA importance measures will not reflect the SSC at all, it would be inappropriate to conclude that the programmatic activity is unimportant, on grounds that the target SSC is not important according to the usual measures.

It is one of the jobs of the Expert Panel to extrapolate from the PRA to draw conclusions about SSCs not modeled in the

PRA. This does not mean that the experts are to impute to the PRA high-level results that were not generated in the analysis; it does mean that if a success path is modeled in the PRA, the experts are justified in reasoning that unmodeled SSCs in that pat[illegible] implicitly invoked. If items were screened from the PRA, the experts need to be aware of the screening proces[illegible] in order to avoid violating the basis for the screening.

b. Description of the Method(s) Acceptable to the Staff for Addressing This Issue

SSCs involved in initiating events: In Maintenance Rule implementation, the licensee will identify SSCs that could cause a reactor trip or an actuation of a safety related system. The Expert Panel should evaluate this list in terms of SSCs that might be affected by the proposed application.

Screened-out events: The only way to address this issue is for the Expert Panel to understand the basis on which screening (if any) was performed, and ascertain whether the credit taken in screening is implicitly conditional upon the proposed application.

Unmodeled components in modeled trains: The Expert Panel looks at detailed drawings of systems that are credited, searching for unmodeled components in these systems. Having identified these, the panel decides whether the components play a role in the safety case, and if so, what level of programmatic resources is appropriate.

Unmodeled SSCs isolating credited systems from other systems: The Expert Panel looks at detailed drawings of systems that are credited in the PRA, searching for interfaces with other systems. Having identified these interfaces, the panel assesses their safety significance and decides what level of programmatic resources is appropriate.

Sequence termination time: The Expert Panel looks not only at drawings but also at procedures to see what equipment are invoked that were not modeled. If these can fail in ways that might prolong the transition to a completely stable shutdown condition, then some consideration may need to be given to allocating performance to these items. The scenarios of interest here are beyond-single-failure but well short of vessel failure. The concern is whether delay in stabilizing the situation can create a window of vulnerability, during which another failure could occur or control of primary conditions could somehow be lost.

c. Acceptance Guidelines:

The Expert Panel is required to affirm that it has:

reviewed the PRA assumption base for instances in which initiators were screened out on the basis of credit for SSCs affected by the application;

reviewed plant operating history for initiating events whose occurrence might have been prevented by the proposed application;

reviewed plant operating history for failures of mitigating system trains as a result of events that might have been prevented by the proposed application;

reviewed detailed drawings for the affected SSCs that were not modeled because they do not normally change state, or components that perform a normally passive function such as isolation of mitigating systems from other systems;

reviewed accident sequence modeling for instances in which early termination of the analysis obscured challenges to affected SSCs that would normally come into play later than the termination point.

Possible dispositions of the above include the following:

the item will not affect initiating event frequency or mitigating system performance under reasonably foreseeable circumstances, and the proposed change is warranted;

the item, although unmodeled, already receives and will continue to receive programmatic attention commensurate with its significance;

the item does not currently receive sufficient programmatic attention, and in future will be subject to tighter controls.

In addition, consideration should be given to modeling items that appear significant in a future update of the PRA.

d. Review Procedures:

Only in exceptional circumstances, or when a decision has been taken to perform an audit, will a reviewer undertake to replicate the search for unmodeled components. Such a search would require access to too many drawings and system notebooks, and the reviewer would be proceeding without the benefit of the intimate acquaintance with the plant that informs the Expert Panel's activities. Here, as in other areas, the reviewer must rely on review of the process, as documented in the formal record of the panel's work.

The reviewer should verify that the documentation positively characterizes how the search was performed, shows what components were identified, and shows how a decision was made about each component. The reviewer should realize that when a component is acknowledged to have safety significance, and plant resource (IST, maintenance, etc.) is allocated to it for that reason (as opposed to a plant availability reason), the commitment may assume legal significance. In particular, credit for that commitment may be used as a reason to justify less commitment elsewhere. Therefore, it needs to be appropriately identified and procedures put in place to ensure continued satisfaction.

e. Evaluation Findings:

The SER should contain language essentially equivalent to the following; exceptions should be noted and discussed.

The panel diligently searched for unmodeled components having safety significance that would warrant consideration of potential benefits of the activity where relaxation has been proposed. This included components that might contribute to initiating event occurrence, mitigating system components that were not modeled in the PRA because their failure was not expected to dominate system failure in the baseline configuration, and components in systems that do not play a direct role in mitigation but that interface with mitigating systems. The panel's process for allocating plant resources or functionally equivalent resources to these components was appropriate. The panel's allocations of these resources are adequately documented and captured as commitments.

B.5 Use of System-Level or Functional Importances

a. Area of Review:

Use of system-level or functional importances can be a valuable tool for overcoming the limitations of single-event importance measures. Single-event importance measures have the potential of dismissing all elements of a system despite the system having a high importance by any reasonable measure. A suitably defined measure of system importance can

help to avoid this pitfall. Conversely, there may be grounds for screening out groups of SSCs, owing to the unimportance of the systems of which they are elements. Here, too, system importance measures would be useful.

There are no widely-accepted definitions of system importance. For front-line systems, one possibility is to define a F-V type measure of system importance as the sum of CDF over sequences involving failure of that system, divided by total CDF. Such a measure would need to be interpreted carefully if the numerator included contributions from failures of that system due to support systems. A Birnbaum-like measure could be defined by quantifying CD sequences involving the system, conditional on its failure, and summing up those quantities. This would provide a measure of how often the system is critical.
For support systems, the situation is more complex. To take a two-division plant as an example, front-line failures can occur as a result of failure of support division A in conjunction with failure of front-line division B. Working with a figure of merit based on total failure of support system would miss contributions of this type.

However, the relative subtlety of quantifying system importance should not be allowed to obscure the qualitative insight that emerges simply from consideration of whether and how systems are invoked in particular scenarios. If a front-line system is credited in success paths, then it is in some sense important, and at least some of its SSCs must also be, in some sense, important, even if a given single-event importance measure does not reflect this. A system that supports such a front-line system must also be important as well. This does not mean that all such systems cannot be candidates for relaxation, but simply that they must not be allowed to escape attention completely.

b. Description of the Method(s) Acceptable to the Staff for Addressing This Issue

Given that a front-line system is credited in the event trees, it must be presumed that some elements of it are, in some sense, important. This does not mean that all components in such systems are presumed to need frequent full programmatic attention; it does mean that all components in system trains credited in the PRA must be explicitly considered by the Expert Panel for full programmatic attention.

c. Acceptance Guidelines:

The use of system/functional measures is encouraged. At a minimum, the Expert Panel should:

identify all systems invoked in plant response, and consider them for programmatic attention;

check to see whether failure of components screened out on the basis that they are elements of unimportant systems could affect a system invoked in plant response.

d. Review Procedures:

The reviewer should first check the Expert Panel documentation for evidence that the panel systematically identified systems as indicated above. The reviewer should then verify that at least some elements of each system are considered significant. If this is not the case, then the reviewer should ascertain what performance is allocated to these items in the PRA, and ascertain whether the level of commitment allocated to these elements is commensurate with that performance level. If a system is important but none of its elements is, this may be grounds for an RAI.

Consider the case of a system that contains many redundant flowpaths. Single-event importance analysis will tend to dismiss the flowpaths one at a time, effectively dismissing the group. The focus of the above guidance is that the redundant flowpaths, considered as a subsystem, are important and deserve some attention, even though conventional importance measures would not highlight them. This does not mean that it is necessary to assign every redundant path to the high risk contributor category. In this example, especially if the paths are essentially similar, it is arguably necessary to

consider common cause failure; a program that addresses common cause failure potential by monitoring component performance may provide more safety benefit than a programmed aimed at detecting an already-failed state in individual components.

e. Evaluation Findings:

The SER should incorporate language substantially equivalent to the following. Exceptions, if any, should be noted and explained.

The Expert Panel process explicitly recognized all systems invoked in plant response to initiating events, and ensured that all SSCs in these systems are considered for programmatic attention in areas (IST, ISI, etc.) appropriate to their performance characteristics and to the level of performance needed from them. All SSCs in these systems were explicitly reviewed by the Expert Panel, which assigned resources to them with due consideration of the role that they play in the system of which they are elements and the importance of the function that this system performs. The panel recognized the need to allocate programmatic resources to at least some divisions of every function modeled. No important function has been missed due to misapplication of single-event importance measures.

Appendix C Determination of Risk Importance of Contributors

a. Area of Review:

The identification of SSCs as potential candidates for relaxation in current requirements can be done in many ways. Component categorization by use of PRA importance measures to classify SSCs into high and low risk contributors is one of the acceptable methods. The results from this importance analysis can then be one of the inputs to the expert panel deliberation process to help determine acceptance of a proposed application using the criteria specified in section II.6.

In addition to the determination of relative risk categorization for input to the Expert Panel, the determination of potential risk contribution from SSCs by PRA importance determination can be useful for several other reasons:

The Fussell-Vesely ,, V) measure can identify SSCs that have relatively large contributions to plant risk. The Risk Reduction Worth (RRW) measure is a measure of the maximum reduction in risk which could be achieved if a given SSC were to be made completely reliable. The FV and RRW measures provide the same insights and are useful in identifying components within the scope of an application that can result in the greatest risk benefit if more resources are allocated to improve their reliability. FV and RRW are also useful for evaluating plant design and procedure improvements, operator training, and for backfitting activities. The Risk Achievement Worth (RAW) and Birnbaum (BM) measures can provide indications of how much the plant risk could increase if a given SSC or group of SSCs were to completely fail. This would be of interest in reliability assurance programs and in inspection and enforcement activities where the control of the SSC reliability and availability is important. The determination of risk importances using an appropriate combination of the above (or other) measures will help in the prioritization of licensee and NRC staff resources when the effects of change of requirements on each individual SSCs have to be determined qualitatively as well as quantitatively.

When performed with a series of sensitivity evaluations, it can identify potential risk outliers by identifying SSCs or cutset elements which could dominate risk for various plant configurations and operational modes, PRA model assumptions, and data and model uncertainties.

Importance evaluations can provide a useful means to identify improvements to current plant practices during the risk-informed application process. Therefore, while the process will identify SSCs where the relaxing of regulations might be justified, importance measures can point out SSCs that are high contributors to risk and where more licensee resources should be focussed. Examples could include identification of more QA for non safety related SSCs, identification of more effective test methods to detect the risk significant failure modes, etc.

The use of risk importance measures compensates for the uncertainty in bottom-line results when comparing the acceptable risk change to the allowed change in risk. Robust categorization (including sensitivity studies) can show that a component will be a low risk contributor for a pre-specified range of data and assumptions used. Therefore, low importance can help justify relaxation of requirements. This is especially important in applications where the change in the performance of equipment before and after the proposed applications is not easily quantified (e.g., in graded QA applications). In such applications, the uncertainty associated with the calculation of a bottom line risk increase would be large, and importance measures can provide added confidence that this increase is acceptable if it can be shown that only SSCs that were low risk contributors are involved in the application.

Importance measures can be used to systematically extend risk insights to SSCs not modeled in the PRA. For example, surrogates from the ranked list can be used for some unmodeled SSCs. HEPs, initiating events, or other SSCs from the ranked list can be used to represent SSCs that are implicitly modeled in the PRA.

b. Description of the Method(s) Acceptable to the Staff for Addressing This Issue:

Acceptable methods and guidelines for risk categorization using PRA importance measures are provided in NUREG-1602.

c. Acceptance Guidelines:

When using risk importance measures to identify SSCs that are low risk contributors, potential limitations of these measures have to be addressed. Therefore, information to be provided to the Expert Panel must include sensitivity studies and/or other evaluations to demonstrate the sensitivity of the risk importance results to the important PRA modeling techniques, assumptions, and data. Issues that have to be considered and addressed when determining low risk contributors are listed below. Acceptance criteria for each issue are also provided.

Truncation limit: The truncation limit should be low enough so that the truncated set of minimal cutsets contain all the significant contributors and their logical combinations for the application in question and be low enough to capture at least 95 percent of the CDF.

Different risk metrics: When determining relative risk contributions, contributions from internal events, external events, and shutdown and low power initiators have to be considered either by use of PRA or by the expert panel process (as detailed in sections II.4.1, II.6.5 and Appendix B). Similarly, risk in terms of both CDF and LERF should be considered.

Multiple component considerations: The aggregate impact of the degradation of multiple components has to be addressed and controlled. The criteria to assure defense in depth and guidelines on evaluating and guarding against multiple degradations, CCFs and removal of multiple controls will address this issue.

Consideration of all allowable plant configurations and maintenance states: The effects of plant configuration should be evaluated as part of the sensitivity and robustness studies. Again, the criteria to assure defense in depth will also help address this issue.

Sensitivity analysis for component data uncertainties: Component categorizations should be carried out using the 5th and 95th percentiles of the SSC unavailability distributions to highlight any SSCs that might become a high risk contributor as a result of the large uncertainty in its unavailability.

Sensitivity analysis for component group failures: Component categorization should be carried out using mean failure rates that have been increased by the generic error factor associated with the component type to address the potential correlated change in the failure rate of a group of components.

Sensitivity analysis for common cause failures: Component categorization should be carried using a wide range of CCF rates to determine the risk impact of modeling assumptions of CCF.

Sensitivity analysis for recovery actions: Component categorization should be carried out without credit in the PRA model for non-proceduralized recovery actions and without credit for repair of failed components to determine the risk impact of non-proceduralized and "uncertain" compensating operator actions.

Each of the above issues is discussed more in detail in NUREG-1602.

In addition to probabilistic risk categorization, risk significance of SSCs must also be evaluated based on deterministic considerations. SSCs that are categorized as low risk contributors using PRA have to be reviewed by an Expert Panel using

criteria and guidelines similar to those discussed in Sections II.6.5 and III.6 5.

d. Review Procedures:

Results from SSC risk categorization can be used directly for identifying SSCs that are high risk contributors (e.g., for the identification of risk outliers, or for the identification of SSCs where more resources should be allocated), however, when risk importance methods are used to group components as low risk contributors, additional evaluations, sensitivity studies and other considerations have to be taken into account. These are summarized below.

Consideration of Truncation Limit

In general truncation limits should be chosen such that at least 95 percent of the CDF or risk is captured. Depending on the PRA level of detail (module level, component level, or piece-part level), this may translate into a truncation limit from 1.0E-12 to 1.0E-8.

In addition, the truncated set of minimal cutsets have to be shown to contain the important application-specific contributors and their logical combinations. This coverage of the contributors by the truncated set can be checked by increasing the failure probabilities or unavailabilities of the contributors (e.g., to 0.5) and regenerating the minimal cutsets.

Consideration of Different Risk Metrics

Importance measures may be calculated based on a portion of the risk (e.g., CDF for internal events and operational mode) or the overall "total" plant risk (CDF and LERF for internal and external events including at-power and shutdown risk). It is critical that the basis for the evaluation of risk contribution be understood by the Expert Panel so that panel deliberations can take the non-modeled initiators and/or modes into account.

Multiple Component Considerations

The aggregate impact of degradation of multiple components on safety should be understood and controlled. Where possible, multiple component importances should be evaluated to identify which combination of events might be risk significant. It should be noted that the concern about multiple component importance measures is also valid for components of different types, as long as they show up in the same cutset. When multiple component importances cannot be readily performed, the review will have to use the defense in depth criteria and guidelines on evaluating and guarding against multiple degradations, CCFs and removal of multiple controls to address this issue.

Consideration for Allowable Plant Configurations and Maintenance States

Plant Technical Specification allow two or more components to be down simultaneously for repair or other activities. The embedded assumption in the TS is that the remaining components provide adequate safety protection. If current commitments on these remaining components are relaxed, their high reliability could not be ensured. To evaluate risk contributions during all allowable plant configurations, sensitivity studies on these configurations have to be performed and results provided to the Expert Panel.

Considerations for Uncertainty Evaluation

The effects of PRA uncertainties have to be addressed to show robustness of the risk categorization results. When possible, a propagation of uncertainty estimates should be performed. However, for component risk categorization, sensitivity analyses could be a substitute for a formal uncertainty evaluation. The following sensitivity analyses should be

performed to demonstrate that results are robust for different plausible assumptions or scenarios.

- **Component-Specific Sensitivity Analyses**

This sensitivity analysis should be carried out to address the failure rate uncertainties of components and their potential impact on categorization. For example, an analysis using the 5th and 95th percentiles of the unavailability distributions of the components could be performed to determine the range of variations in FV measures. The relative risk contributions from components with large uncertainties (such as check valves) could vary substantially, and these results should be considered by the Expert Panel.

- **Sensitivity Analyses for a Component Group**

This sensitivity analysis should be carried out to address the correlated change in a failure rate of a group of components as a result of the proposed application or from such causes as aging and wear. For a group of components (e.g., breakers), an increase in the mean failure rate of all selected components with a generic error factor associated with the component type could result in risk impacts that have to be considered by the Expert Panel.

- **Sensitivity Analysis for Common-Cause Failures (CCFs)**

CCFs are modeled in PRAs to account for dependent failures of redundant components within a system. Dependencies among similar components performing redundant functions but across systems (in two different systems) are not currently modeled in PRAs. Component-level importance measures (e.g., RAW, RRW, and FV) are typically calculated based on the combined effect of all basic PRA events. Such component importance measures would account for the direct risk contributions from associated basic component events, such as failure to start and failure to run, and indirect contributions through the impact on the probability of other basic events (such as human errors, recovery actions, and most importantly CCFs). Therefore, a component may be ranked as a high risk contributor mainly because of its contribution to CCFs, or a component may be ranked as low risk contributor mainly because it has negligible or no contribution to CCFs. In RIR, removing or relaxing requirements may increase the CCF contribution, thereby changing the risk impact of an SSC. Therefore, sensitivity studies using different CCF modeling assumptions will highlight the robustness of risk categorization results to CCF.

- **Sensitivity Analysis for Recovery Actions**

PRAs typically model recovery actions especially for dominant accident sequences. Quantification of recovery actions typically depends on the time available for diagnosis and performing the action, training, procedure, and knowledge of operators. There is a certain degree of subjectivity involved in estimating the success probability for the recovery actions. The concerns in this case stem from situations where very high success probabilities are assigned to a sequence, resulting in related components being ranked as low risk contributors. Furthermore, it is not desirable for the categorization of SSCs to be impacted by recovery actions that sometimes are only modeled for the dominant scenarios. Sensitivity analyses can be used to show how the SSC categorization would change if all recovery actions were removed.

e. Evaluation Findings:

The reviewer verifies that the information provided to the Expert Panel on the determination of risk importance of contributors is robust in terms of the "uncertainty" issues like common cause failure modeling and modeling of human reliability.