

July 1, 1997

Mr. Christian A. Sanna
American Society of Mechanical Engineers
Nuclear Department M/S 13E 345
East 47th Street
New York, New York 10017-2392

Dear Mr. Sanna;

At the last Nuclear Quality Assurance (NQA) committee meeting, I offered to provide you with a copy of the Nuclear Regulatory Commission (NRC) risk-informed guidance documents for review by NQA committee members. On June 25, 1997, a Federal Register Notice (FRN) announced the availability of the guidance documents, including guidance for graded QA, for public comment. The FRN describes how to access the guidance documents through electronic means. The FRN also delineates a specific set of questions for which the NRC requests feedback from the public and outlines how comments should be transmitted to the NRC. The public comment period will expire on September 23, 1997.

Please find enclosed a copy of the associated press release, the FRN, and a set of the risk-informed guidance documents. Your members should be aware that for applications such as graded QA the composite set of guidance contained in Draft Regulatory Guide DRG-1061 and its companion Standard Review Plan Chapter 19, as well as DRG-1064 for Graded QA is considered applicable.

If there are any general questions, you can contact the individuals identified in the FRN or the press release. For specific questions regarding graded QA, you can contact either myself at (301) 415-1017 or Mr. Robert Gramm at (301) 415-1010.

Sincerely,

Original signed by: Suzanne C. Black
Suzanne C. Black, Chief
Quality Assurance and Maintenance Branch
Division of Reactor Controls
and Human Factors
Office of Nuclear Reactor Regulation

Enclosures: As Stated

DISTRIBUTION:

Central Files
PUBLIC
JCraig, RES

HQMB R/F (w/o guidance documents)
OGormley, RES
WBelke, NMSS (w/o guidance documents)

DF031/
L-4-1 PT 50
QA
x OIRM-6 meeting

DOCUMENT NAME: G:ASME.LTR

To receive a copy of this document, indicate in the box: "C" = Copy without attachment/enclosure "E" = Copy with attachment/enclosure "N" = No copy

| | | | | | | | | | |
|--------|--------------|-------------------------------------|--------------|-------------------------------------|---------|--|---------|--|---------|
| OFFICE | SC:HQMB:DRCH | <input checked="" type="checkbox"/> | BC:HQMB:DRCH | <input checked="" type="checkbox"/> | | | | | |
| NAME | RAGramm:cct | | SCBlack | | | | | | |
| DATE | 06/27/97 | | 06/27/97 | | 06/ /97 | | 06/ /97 | | 06/ /97 |

9707020283 970701
PDR REGGD
GENERAL PDR

97-129
NRC FILE CENTER COPY

Nuclear Regulatory Commission

Office of Public Affairs

Washington DC 20555

Telephone: 301/415-8200 -- E-mail: opa@nrc.gov

No. 97-096

June 25, 1997

NRC SEEKS PUBLIC COMMENT ON DRAFT GUIDANCE FOR POWER REACTOR LICENSEES ON USING RISK INFORMATION FOR LICENSING BASIS CHANGES

The Nuclear Regulatory Commission is seeking public comment on drafts of four regulatory guides, three Standard Review Plan sections, and a NUREG document designed to help power reactor licensees use risk information to make changes in their plants' licensing bases.

On August 16, 1995, the NRC staff published in the Federal Register a final policy statement on the use of probabilistic risk assessment methods

(a way of estimating the risk associated with nuclear power plant accidents). It was the Commission's intent that risk information be used to enhance safety decision-making, make more efficient use of agency resources and reduce unnecessary burdens on its licensees.

To implement the Commission's policy on the use of risk information in the regulatory process, NRC has developed specific documents that are available for comment. These are:

Draft regulatory guide DG-106, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis," and its companion SRP, Chapter 19.

Draft regulatory guide DG-1062, "An Approach for Plant-Specific Risk-Informed Decision Making: Inservice Testing," and its companion SRP, Chapter 3.9.7.

Draft regulatory guide DG-1064, "An Approach for Plant-Specific, Risk-Informed Decision Making: Graded Quality Assurance."

Draft regulatory guide DG-1065, "An Approach for Plant-Specific, Risk-Informed Decision Making: Technical Specifications" and its companion SRP, Chapter 16.1, and

Draft NUREG-1602, "Use of PRA in Risk-Informed Applications."

To facilitate public comment, the NRC staff intends to conduct a workshop during the comment period to explain the draft documents and answer questions. The time, location and agenda will be published in a future issue of the Federal Register and announced in the NRC's public meeting bulletin board.

The request for public comment has been published in the June 25 edition of the Federal Register. Copies of the draft regulatory guides, Standard Review Plan sections and NUREG report may be obtained by contacting Mark Cunningham, Office of Nuclear Regulatory Research, T10-E50, U.S. Nuclear Regulatory Commission, Washington, D.C. 20555-0001; telephone (301) 415-6189.

Written comments can be mailed to David L. Meyer, Chief, Rules Review and Directives Branch, Office of Administration, Mail Stop T-6D59, U.S. Nuclear Regulatory Commission, Washington, D.C. 20555-0001. Written comments may also be hand-delivered to the NRC at 11545 Rockville Pike, Rockville, Maryland, between 7:45 a.m. and 4:15 p.m. on normal Federal workdays.

<ARTICLE>

Date="06/25/97"

Citation="62 FR 34321"

Group="energy"

Typ="NOTICE"

Department="NUCLEAR REGULATORY COMMISSION"

Agency="NUCLEAR REGULATORY COMMISSION"

Subject="Use of PRA in Plant Specific Reactor Regulatory Activities: Proposed Regulatory Guides, Standard Review Plan
<HEADER>

NUCLEAR REGULATORY COMMISSION

Use of PRA in Plant Specific Reactor Regulatory Activities:
Proposed Regulatory Guides, Standard Review Plan Sections, and
Supporting NUREG

AGENCY: Nuclear Regulatory Commission.

ACTION: Notice of availability.

</HEADER>

NUCLEAR REGULATORY COMMISSION

Use of PRA in Plant Specific Reactor Regulatory Activities:
Proposed Regulatory Guides, Standard Review Plan Sections, and
Supporting NUREG

AGENCY: Nuclear Regulatory Commission.

ACTION: Notice of availability.

+

SUMMARY: The Nuclear Regulatory Commission has issued for public comment drafts of four regulatory guides, three Standard Review Plan Sections, and a NUREG document. These issuances follow Publication of the Commission's August 16, 1995 (60 FR 42622) Policy statement on the Use of PRA Methods in Nuclear Regulatory Activities. The NRC has developed draft guidance for power reactor licensees on acceptable methods for using probabilistic risk assessment (PRA) information and insights in support of plant-specific applications to change the current licensing basis (CLB). The use of such PRA information and guidance is voluntary. To facilitate comment, the Commission intends to conduct a workshop during the comment period to explain the draft documents and answer questions. The exact time, location and agenda will be announced in a future issue of the Federal Register. Section VI of this notice provides additional information on the scope, purpose and topics for discussion at the workshop.

DATES: Comment period expires September 23, 1997. Comments received after this date will be considered if it is practical to do so, but the Commission is able to assure consideration only for comment received on or before this date.

ADDRESSES: Mail written comments to: David L. Meyer, Chief, Rules and Directives Branch, Office of Administration, Mail Stop T-6D59, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

In addition to written comments, please (1) attach a diskette containing your comments, in either ASCII text or Wordperfect format (Version 5.1 or 6.1), or (2) submit your comments electronically via the NRC Electronic Bulletin Board on FedWorld or the NRC's Interactive Rulemaking Website.

---- page 34322 ----

Deliver comments to 11545 Rockville Pike, Rockville, Maryland, between 7:30am and 4:15pm, Federal workdays.

Copies of the draft regulatory guides, standard review plan sections and NUREG are available for inspection and copying for a fee at the NRC Public Document Room, 2120 L Street NW, (Lower Level).

Washington, DC 20555-0001. A free single copy of these draft documents to the extent of supply, may be requested by writing to Distribution Services, Printing, Graphics and Distribution Branch, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by Fax to (301) 415-5272. Electronic copies of the draft document are also accessible on the NRC's Interactive Rulemaking Website through the NRC home page (<http://www.nrc.gov>). This site provides the same access as the FedWorld bulletin board, including the facility to upload comments as files (any format), if your web browser supports the function.

For more information on the NRC bulletin boards call Mr. Arthur Davis, Systems Integration and Development Branch, NRC, Washington, DC 20555-0001, telephone (301) 415-5780; e-mail AXD3@nrc.gov. For information about the Interactive Rulemaking Website, contact Ms. Carol Gallagher, (301) 415-5905; e-mail CAG@nrc.gov.

The NRC subsystems on FedWorld can be accessed directly by dialing the toll free number: 1-800-303-9672. Communication software parameters should be set as follows: parity to none, data bits to 8, and stop bits to 1 (N,8,1). Using ANSI or VT-100 terminal emulation, the NRC NUREGs and Reg Guides for Comment subsystem can then be accessed by selecting the "Rule Menu" option from the "NRC Main Menu." For further information about options available for NRC at FedWorld, consult the "Help/Information Center" from the "NRC Main Menu." Users will find the FedWorld online User's Guides particularly helpful. Many NRC subsystems and databases also have a "Help/Information Center" option that is tailored to the particular subsystem.

The NRC subsystem on FedWorld can also be accessed by a direct dial phone number for the main FedWorld BBS, 703-321-3339, or by using Telnet via Internet, fedworld.gov. If using 703-321-3339 to contact FedWorld, the NRC subsystem will be accessed from the main FedWorld menu by selecting the "Regulatory, Government Administration and State Systems," then selecting "Regulatory, Information Mail." At that point, a menu will be displayed that has an option "U.S. Nuclear Regulatory Commission" that will take you to the NRC Online main menu. The NRC Online area also can be accessed directly by typing "/go nrc" at a FedWorld command line. If you access NRC from FedWorld's main menu, you may return to FedWorld by selecting the "Return to FedWorld" option from the NRC Online Main Menu. However, if you access NRC at FedWorld by using NRC's toll-free number, you will have full access to all NRC systems but you will not have access to the main FedWorld system.

If you contact FedWorld using Telnet, you will see the NRC area and menus, including the Rules menu. Although you will be able to download documents and leave messages, you will not be able to write comments or upload files (comments). If you contact FedWorld using FTP, all files can be accessed and downloaded but uploads are not allowed; all you will see is a list of files without descriptions (normal Gopher look). An index file listing all files within a subdirectory, with descriptions, is included. There is a 15-minute time limit for FTP access.

Although FedWorld can be accessed through the World Wide Web, like FTP that mode only provides access for downloading files and does not display the NRC Rules menu.

FOR FURTHER INFORMATION CONTACT: Mark Cunningham, Office of Nuclear Regulatory Research, MS: T10-E50, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, (301) 415-6189.

SUPPLEMENTARY INFORMATION:

I. Background

On August 16, 1995, (60 FR 42622) the Commission published in the Federal Register a final policy statement on the Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities. The policy statement included the following policy regarding expanded NRC use of PRA:

1. The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.
2. PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices. Where appropriate, PRA should be used to support

proposals for additional regulatory requirements in accordance with 10 CFR 50.109 (Backfit Rule). Appropriate procedures for including PRA in the process for changing regulatory requirements should be developed and followed. It is, of course, understood that the intent of this policy is that existing rules and regulations shall be complied with unless these rules and regulations are revised.

3. PRA evaluations in support of regulatory decisions should be as realistic as practicable and appropriate supporting data should be publicly available for review.

4. The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgments on the need for proposing and backfitting new generic requirements on nuclear power plant licensees.

It was the Commission's intent that implementation of this policy statement would improve the regulatory process in three areas:

1. Enhancement of safety decision making by the use of PRA insights,

2. More efficient use of agency resources, and

3. Reduction in unnecessary burdens on licensees.

In parallel with the development of Commission policy on uses of risk assessment methods, the NRC developed an agency-wide implementation plan for application of probabilistic risk assessment insights within the regulatory process (SECY-95-079). This implementation plan included tasks to develop Regulatory Guides (RG) and Standard Review Plans (SRP) in the areas of:

--General guidance,

--Inservice inspection (ISI),

--Inservice testing (IST),

--Technical specification (TS), and

--Graded quality assurance (GQA).

These RGs and SRPs are intended to help implement the Commission's August 1995 policy on the use of risk information in the regulatory process and to provide an acceptable approach for power reactor licensees to prepare and submit and NRC staff to review applications for proposed plant-specific changes to the current licensing basis that utilize risk information. Currently, draft RGs/SRPs have been developed and are ready for comment in the areas of general guidance, IST and TS. A draft RG for GQA has also been developed and is ready for comment. No SRP has been developed for GQA, since the NRC staff will utilize its inspection process

---- page 34323 ----

in the GQA area. In addition, the NRC has prepared draft NUREG-1602, "Use of PRA in Risk-Informed Applications," to provide reference information for licensees and NRC staff and it is also ready for public comment. Each of these documents is discussed in more detail below.

II. An Overview of Draft RGs, SRPs, and NUREG-1602

The specific documents available for comment are:

+ Draft regulatory guide DG 1061, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis," and its companion SRP, Chapter 19,

+ Draft regulatory guide DG-1062 "An Approach for Plant-Specific, Risk-Informed, Decision Making: Inservice Testing" and its companion SRP, Chapter 3.9.7,

+ Draft regulatory guide DG-1064, "An Approach for Plant-Specific, Risk-Informed Decision Making: Graded Quality Assurance,"

+ Draft regulatory guide DG-1065, "An Approach for Plant-Specific, Risk-Informed Decision Making: Technical Specifications" and its companion SRP, Chapter 16.1, and

+ Draft NUREG-1602, "Use of PRA in Risk-Informed Applications."

The purpose of the RGs and SRPs is to provide guidance to power reactor licensees and NRC staff reviewers on an acceptable approach for utilizing risk information to support requests for changes in a plant's CLB. The purpose of NUREG-1602 is to provide reference information useful in making decisions on the scope and attributes of PRA. The RGs describe an alternate means by which licensees can propose plant-specific CLB changes under 10 CFR Part 50. Adopting the approach of these RGs is voluntary. Licensees submitting applications for changes to their CLB may use this approach or an alternative equivalent

approach. To encourage the use of risk information in such applications, the staff intends to give priority to applications for burden reduction that use risk information as a supplement to traditional engineering analyses, consistent with the intent of the Commission's policy. All applications that improve safety will continue to receive high priority.

The general RG/SRP have been developed to provide an overall framework and guidance that is applicable to any proposed CLB change where risk insights are used to support the change. The application-specific RGs/SRPs (i.e., IST, TS, GQA) build upon and supplement the general guidance for proposed CLB changes in their respective technical areas. Each application-specific RG/SRP references the general RG/SRP, states that the general guidance is applicable and provides additional guidance specific to the technical area being addressed.

The guidance provided in these documents is designed to encourage licensees to use risk information by defining an acceptable framework for the use of risk information on a plant-specific basis, and by promoting consistency in PRA applications. It is expected that the long-term use of risk information in plant-specific licensing actions will result in improved safety by focusing attention on the more risk significant aspects of plant design and operation. The draft guidance provides flexibility to licensees by allowing them to define the scope of the analysis required to support their proposed change and to perform appropriate analysis to justify proposed changes to the plant's CLB.

In conjunction with developing these RGs and SRPs, the staff has also been working with several licensees on pilot applications of risk informed regulation in the technical areas listed above. The knowledge gained to date in interacting with licensees on these pilot applications has been used to help define the content and guidance contained in these RGs/SRPs. Additional interactions are expected over the next several months as work on these pilot applications continues and licensees and other interested persons have an opportunity to review the draft RGs/SRPs. The results of these additional interactions will be factored into the final RGs/SRPs.

III. Policy Issues

On May 15, 1996, the Commission requested the staff to identify and recommend resolution of the following four policy issues associated with risk-informed changes to a plant's CLB:

- + The role of performance-based regulation,
- + Plant-specific application of safety goals,
- + Risk neutral vs. increases in risk,
- + implementation of changes to risk-informed IST and ISI requirements.

On January 22, 1997, the Commission provided the following guidance on these issues:

A. The Role of Performance-Based Regulation in the PRA Implementation Plan

The Commission instructed the staff to include, where practical, performance-based strategies in the implementation of the risk-informed regulatory process. Furthermore, the Commission indicated that application of performance-based approaches should not be limited to risk-informed initiatives and that performance-based initiatives that do not explicitly reference criteria derived from PRA insights should not be excluded from consideration. The Commission also instructed the staff to include in the PRA Implementation Plan, or in a separate plan, how these performance-based initiatives will be phased into the overall regulatory improvement and oversight program and to solicit input from industry on (or develop on its own) additional performance-based objectives which are not amenable to probabilistic risk analysis but could be ranked according to, for example, a relative hazards analysis, and phase in these initiatives.

B. Plant-Specific Application of Safety Goals

The Safety Goals policy statement, issued by the Commission in 1986, established two qualitative safety goals to help ensure that nuclear power plant operations do not significantly increase risk to individuals or to the society. The policy statement also defined two Quantitative Health Objectives (QHO) for use "in determining achievement of the qualitative goals." Subsequently, the Commission approved for use two subsidiary objectives derived from the Safety Goal QHOs, one on core-damage frequency and one on containment performance,

for use in assessing reactor designs for generic actions. The Commission approved the Safety Goals for use in generic actions with the intent that they would define "how safe is safe enough" in deciding how far to go when proposing safety enhancements.

The staff has considered the need for risk guidelines to support regulatory decision-making in plant-specific circumstances, recognizing that the use of risk information remains complementary to traditional engineering analysis and judgment. Specifically, the staff recommended the development of guidelines for plant-specific applications, derived from the Commission's current Safety Goals and/or subsidiary objectives and requested Commission approval.

The Commission tentatively approved the plant-specific application of safety goals and/or their subsidiary objectives.

C. Risk Neutral vs. Increases in Risk

This policy issue is related to whether to allow small increases in calculated plant risk in approving a change to the CLB.

---- page 34324 ----

The Commission approved small increases in risk under certain conditions, for proposed changes to a plant's CLB. In giving this approval the Commission noted that the terms "small" and "under certain conditions" require more precise definition. The staff was requested to provide a sound rationale for judging small increases and provide for explicit consideration of uncertainties. Criteria for judging small increases in risk should be considered in the context of maintaining reasonable assurance that there is no undue risk to public health and safety.

Moreover, the Commission asked the staff that, in its development of risk-informed guidance and review of applications regarding risk-informed initiatives, to evaluate all safety impacts of proposed changes in an integrated manner including the use of risk insights to identify areas where requirements should be increased or improvements could/should be implemented.

D. Implementation of Changes to Risk-Informed IST and ISI Requirements

This policy issue is related to identifying a means for implementing risk-informed inservice inspection and testing programs until rulemaking is complete. The alternatives are to treat proposed changes as exceptions to 10 CFR 50.55(a) or to treat them as authorized alternatives under the current rule. The Commission approved risk informed ISI and IST changes as authorized alternatives under 10 CFR 50.55a(a)(3)(i) to approve the pilot plant applications, provided appropriate findings can be made. In addition, the Commission instructed the staff that in cases where the findings necessary to approve the alternative cannot be made, then the use of exemptions should be considered.

IV. Structure, Guidelines and Rationale for RGs/SRPs

The approach described in each of the RGs/SRPs has four basic steps. These are:

- Define the proposed change;
- Perform an integrated engineering analysis (which includes both traditional engineering and risk analysis) and use of an integrated decision process;
- Monitoring and feedback to verify assumptions and analysis; and
- Document and submit proposed change.

Five fundamental safety principles are described which should be met in each application for a change in the CLB. These principles are:

- The proposed change meets the current regulation. This principle applies unless the proposed change is explicitly related to a requested exemption or rule change (i.e., a 50.12 "specific exemption" or a 2.802 "petition for rulemaking");
- Defense-in-depth is maintained;
- Sufficient safety margins are maintained;
- Proposed increases in risk, and their cumulative effect, are small and do not cause the NRC Safety Goals to be exceeded;
- Performance-Based implementation and monitoring strategies are proposed that address uncertainties in analysis models and data and provide for timely feedback and corrective action.

These principles represent fundamental safety practices that the staff believes must be retained in any change to a plant's CLB to maintain reasonable assurance that there is no undue risk to public health and safety. Each of these principles is to be considered in the integrated engineering analysis and decision-making process.

The guidelines for assessing risk proposed in the RGs/SRPs are derived from the Commission's Safety Goal Quantitative Health Objectives (QHOs). Specifically, the subsidiary objectives of Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) are used as the measures of risk against which changes in the CLB will be assessed, in lieu of the QHOs themselves, which require level 3 PRA information (offsite health effects). These were chosen to simplify the scope of PRA analysis needed, to avoid the large uncertainties associated with level 3 PRA analysis, and to be consistent with previous Commission direction to decouple siting from plant design.

The values used in the RGs/SRPs as guidelines for CDF and LERF were selected to be consistent with the Safety Goal QHOs and previous Commission guidance. Specifically, a CDF value of $10^{-4}/\text{RY}$ is proposed as the guideline where further increases in CDF would not be acceptable (i.e., plants with $\text{CDF} \geq 10^{-4}/\text{RY}$ would be expected to propose changes that result in CDF decreases or are neutral). The CDF value of $10^{-4}/\text{RY}$ is the value endorsed by the Commission in a Staff Requirements Memorandum dated June 15, 1990, as a benchmark objective for accident prevention. For plants with $\text{CDFs} < 10^{-4}/\text{RY}$, guidelines are proposed on changes in CDF (DELTA CDF) that ensure increases in risk from CLB changes are made in small steps and that increased NRC management attention is provided for proposed changes that approach the guidelines (i.e., CDFs in the range $10^{-5}/\text{RY}$ to $10^{-4}/\text{RY}$ and $\text{DELTA CDF} > 10^{-6}/\text{RY}$). The use of small steps is consistent with a measured approach (allowing time for monitoring, feedback and corrective action) and the values chosen for DELTA CDF are consistent with the Commission's Regulatory Analysis Guidelines (NUREG/BR-0058, Rev. 2).

The guidelines on LERF are derived from the Commission's Safety Goal QHO for early fatality risk. A LERF value of $10^{-5}/\text{RY}$ is proposed as the guideline where further increases in LERF would not be acceptable (i.e., plants with a $\text{LERF} \geq 10^{-5}/\text{RY}$ would be expected to propose changes that result in LERF decreases or are neutral). Similar to CDF, a range is proposed where increased NRC management attention is required if LERF approaches the guideline (i.e., LERF in the range of $10^{-6}/\text{RY}$ to $10^{-5}/\text{RY}$). The value of $10^{-5}/\text{RY}$ for the LERF guideline corresponds to that value, estimated from existing PRA results, necessary to ensure that the early-fatality QHO would be met without undue conservatism. In effect, the guideline value for LERF is a surrogate for the Commission's QHO on early fatality risk. Guidelines for changes in LERF (DELTA LERF) are used that limit increases in risk to small values (i.e., $\text{DELTA LERF} < 10^{-6}/\text{RY}$) to ensure that increases are made in small increments, are consistent with the Regulatory Analysis Guidelines and, similar to DELTA CDF , require increased management attention when they approach the guideline value (i.e., DELTA LERF in the range of $10^{-7}/\text{RY}$ to $10^{-6}/\text{RY}$).

The CDF/ DELTA CDF and LERF/ DELTA LERF guidelines are intended for comparison with a full-scope PRA (i.e., full power, low power and shutdown conditions and internal and external events). It is expected that the cumulative impact of previous CLB changes will also be reflected in the PRA. However, it is recognized that less than full-scope PRA analysis will likely be acceptable for many proposed CLB changes and the RG/SRP guidance is intended to allow licensees flexibility to do analyses appropriate for their proposed change and to allow the use of qualitative factors in the decision process. In addition, mean values of CDF and LERF are to be compared against the guidelines. However, when a proposed change is closer to the guidelines, a more comprehensive uncertainty and sensitivity analysis is expected that includes the consideration of qualitative factors. Only general guidelines on uncertainty/sensitivity analyses are included in the RGs/SRPs to allow

---- page 34325 ----

licensees flexibility to provide analyses appropriate for their specific application.

Monitoring and feedback strategies are to be utilized in implementing the proposed CLB change to help verify assumptions and analysis and to allow for corrective action should performance be less

than assumed in the analysis. In addition, NRC expects licensees to identify how and where their proposed changes will be documented as part of the plant's CLB. This should include documentation that clearly establishes the basis for the change, ensures that commitments are known and provides sufficient documentation to allow inspection and enforcement, if appropriate. Related to the above, since these RGs/SRPs allow the use of risk information and monitoring programs to support CLB changes associated with safety related systems, structures and components (SSCs), it is reasonable to expect that the quality of these analyses and monitoring programs should be consistent with the quality of other analyses and activities associated with safety related SSCs (i.e., 10 CFR part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"). Accordingly, DG-1061 includes guidance regarding quality assurance, including that associated with the PRA, that ensures the pertinent requirements of 10 CFR part 50, Appendix B are met. In addition, the draft RGs/SRPs use the definition of CLB that is currently in 10 CFR part 54 "License Renewal." Although not officially incorporated in 10 CFR part 50, this definition is considered appropriate for use in these RGs/SRPs.

As mentioned above, the draft guidance encourages licensees to utilize risk insights to improve safety, as well as to propose reductions of unnecessary burdens. The Commission's Safety Goals, their subsidiary objectives and Regulatory Analysis Guidelines have been used to derive guidelines for judging the acceptability of any calculated risk increases associated with the proposed CLB change. In this regard, a measured approach to reviewing and accepting changes to CLBs that increase risk has been taken. Specifically, the guidelines used correspond to small calculated increases in risk. In theory, one could construct an even more generous regulatory framework for consideration of those risk-informed changes which may have the effect of increasing risk to the public. Such a framework would include, of course, assurance of continued adequate protection (that level of protection of the public health and safety which must be reasonably assured regardless of economic cost), but it could also include provision for possible elimination of all measures not needed for adequate protection which either do not contribute to a substantial reduction in overall risk or result in continuing costs which are not justified by the safety benefits. However, a more restrictive practice has been used which would permit only small increases in risk, and then only when it is reasonably assured, among other things, that sufficient defense in depth and safety margins are maintained. This practice is used because of the uncertainties in PRA and to account for the fact that safety issues continue to emerge regarding design, construction, and operational matters notwithstanding the maturity of the nuclear power industry. In addition, limiting risk increases to small values is considered prudent until such time as experience is obtained with the methods and applications discussed in the RGs/SRPs.

V. Comments

The staff is soliciting comments related to the guidance described in the draft RGs, SRPs and NUREG-1602. Comments submitted by the readers of this FRN will help ensure that these draft documents have appropriate scope, depth, quality, and effectiveness. Alternative views, concerns, clarifications, and corrections expressed in public comments will be considered in developing the final documents.

VI. Workshop

The Commission intends to conduct a workshop to discuss and explain the material contained in the draft guides, SRPs and NUREG-1602, and to answer questions and receive comments and feedback on the proposed documents. The purpose of the workshop is to facilitate the comment process. In the workshop the staff will describe each document, its basis and solicit comment and feedback on their completeness, correctness and usefulness. Since these documents cover a wide range of technical areas, many topics will be discussed. Listed below are topics on which discussion and feedback are sought at the workshop:

(1) Overall Approach

(A) Is it appropriate to apply the Commission's Safety Goals and their subsidiary objectives on a plant specific basis?

(B) Is it appropriate to allow, under certain conditions, changes to a plant's CLB that increase CDF and/or LERF?

(C) Is the level of detail in the guidance contained in the proposed Regulatory Guides and SRPs clear and sufficient, or is more

- detailed guidance necessary? What level of detail is needed?
- (D) Are the four elements of the risk-informed process described in the Reg Guides and SRPs clear and sufficient?
- (E) Is the guidance on the treatment of uncertainties clear and sufficient, or is additional guidance necessary? What additional guidance is needed?
- (F) Is guidance on the acceptability and treatment of temporary changes in the CLB (i.e., temporary changes in risk) needed? If so, what guidance and acceptance guidelines should be included? Should the guidance be different for full-power operation vs a shutdown condition?
- (G) Is it appropriate to use the definition of "current licensing basis" included in 10 CFR 54 "License Renewal," in these RGs/SRPs? What other definition would be more appropriate?
- (H) Should licensees be required to submit risk information in support of proposed changes to their CLB?
- (I) Are the guidelines for quality described in DG-1061 sufficient to ensure appropriate quality in those activities that support proposed changes to the CLB for safety related systems, structures and components? Are the appropriate provisions from 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants" applied to the PRA?
- (J) Should a licensee's PRA be required to be included in the NRC's docket file and updated as necessary to reflect previous changes and recent operating experience?
- (K) What other areas, besides graded QA, Tech Specs, IST and ISI could this process and these guidelines be applied to?

(2) Engineering Evaluation

- (A) Are the proposed safety principles clear and sufficient? What should be clarified and/or added?
- (B) Is sufficient guidance provided regarding the intent, scope, and level of detail requested in the submittal with respect to the evaluation of the safety principles? What should be added? For example:
 1. Should there be different guidance on defense-in-depth for those items analyzed in the PRA versus those not analyzed? What should the differences be?
 2. Should there be quantitative guidelines for determining the sufficiency of defense-in-depth and safety margins?

---- page 34326 ----

- (C) Is the guidance associated with the probabilistic analysis sufficient? For example:
 1. Is additional guidance on the use of qualitative risk evaluations necessary? What additional guidance would be appropriate?
 2. Are the proposed acceptance guidelines for CDF and LERF and changes in CDF and LERF appropriate? Are they too restrictive or too liberal? What guidelines would be more appropriate?
 3. Is more specific or less detailed guidance needed on comparison of PRA results with the CDF and LERF and the DELTACDF and DELTALERF guidelines?
 4. Should there be additional guidance on the number of proposed risk increases which can be submitted in any given year?
 5. Should there be separate LERF guidelines for PWRs and BWRs? What should they be?
 6. Should there be separate LERF guidelines for shutdown conditions/external events? What should they be?
 7. Should there be a guideline on long term release frequency to supplement LERF? What should it be based upon?
 8. Is the guidance in Appendix B of DG-1061 for estimating LERF sufficient? What else is needed? (It should be noted that the staff intends to expand this guidance to cover shutdown conditions and external events).
 9. Should there be acceptance guidelines for the use of PRA level 3 (segment of PRA that includes estimation of consequences/health effects and risk to the public) information? What guidelines would be appropriate?
 10. Should the acceptance guidelines specify a confidence level that the PRA results should meet when being compared to the risk guidelines? What is an appropriate confidence level?
 11. Should a confidence level or uncertainty level be used to define the "management attention" region in, lieu of a CDF and LERF range?

(3) Performance Monitoring and Feedback

(A) Should the use of performance monitoring be more widely applied in regulation and regulatory practice, or is it sufficient to implement it through the elements described in the proposed Regulatory Guides?

(B) Is performance monitoring and feedback an appropriate element of the risk-informed process? Should it be used to a greater or lesser degree?

(C) Is the guidance on performance monitoring and feedback clear and sufficient? What should be improved?

(4) Graded Quality Assurance Regulatory Guide (DG-1064)

(A) Is the approach for determining the safety-significance of plant SSCs appropriate? Is it sufficient to identify high and low safety significant categories? Is the amount of risk analysis overly burdensome relative to the potential benefits?

(B) Is the guidance in the proposed regulatory guide regarding the content of QA programs for low safety significant SSCs appropriate? What additional guidelines are needed, and/or what portions of the proposed guidelines should be deleted?

(C) Are there any quantitative data that can be used to assess the risk impact (i.e., CDF or LERF) of reducing QA controls on equipment performance?

(D) Is the proposed scope of graded QA, that includes safety-related and other important plant equipment as covered by the Maintenance Rule, appropriate?

(E) Is the guidance on equipment-performance-monitoring strategies sufficient?

(F) Is the guidance sufficient regarding the QA controls for safety-significant, but non-safety-related, equipment that should be included in the licensee's QA program? What guidance should be included?

(G) Should the guidance allow for further removal of QA requirements? In what areas should this be done and what guidance would be appropriate? For example, is it appropriate for a graded QA program to eliminate all requirements associated with some of the 18 criteria specified in 10 CFR part 50, Appendix B?

(5) Technical Specifications Regulatory Guide (DG-1065) and SRP

(A) Are the proposed acceptance guidelines on incremental conditional core damage probability and incremental conditional large early release probability from a single AOT change (5E-07 and 5E-08, respectively) appropriate?

(B) Should there be a guideline on maximum conditional CDF/LERF during an AOT? What should it be?

(6) Inservice Testing Regulatory Guide (DG-1062) and SRP

(A) PRA models of component unavailability typically use a parameter λ (λ) to characterize the component's failure rate, and this parameter is often considered to be a constant value. Is the assumption of constant value for λ realistic? What different values might be more realistic and what evidence (data) supports the alternate values?

(B) Is it appropriate, as part of a risk-informed program, to require licensees to look outside the ASME code boundary and identify candidate components for testing and then apply ASME criteria to the conduct of those tests? What is a reasonable way to deal with relatively high-risk components that are not part of a currently prescribed IST program?

(C) Is it appropriate to use the "other acceptable methods" provision of 10 CFR 50.55a to implement changes to the CLB?

(7) NUREG-1602

(A) Draft NUREG-1602 provides reference material on the scope and quality of a PRA. Is the information in draft NUREG-1602 complete and correct? Is it useful as reference material in making assessments on an application specific basis on the scope and quality of the risk assessment to support that particular application? How could it be improved? For example, should it specify acceptable PRA methods?

(B) Would draft NUREG-1602 be useful as a starting point to develop a national consensus standard on PRA? What would be needed?

(C) Is a national consensus standard on PRA needed or desirable?

- These draft regulatory guides contain information collections that
- are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et
- seq.). These regulatory guides will be submitted to the Office of
- Management and Budget for review and approval of the information
- collections before the final guides are published.

VIII. Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, an information collection unless it displays a currently valid OMB control number.

Dated at Rockville, Maryland, this 13th day of June, 1997.

For the Nuclear Regulatory Commission,
John C. Hoyle,
Secretary of the Commission.
[FR Doc. 97-16072 Filed 6-18-97; 8:45 am]
BILLING CODE 7590-01-P

The Contents entry for this article reads as follows:

Probabilistic risk assessment methods; use in nuclear regulatory
activities; proposed regulatory guides availability and comments
request, 34321
</ARTICLE>



U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

March 1997
Draft DG-1061

DRAFT REGULATORY GUIDE

Contact: M. A. Cunningham (301)415-6189

**An Approach for Using Probabilistic Risk Assessment in Risk-Informed
Decisions on Plant-Specific Changes to the Current Licensing Basis**

Draft for Comment

March 28, 1997

This regulatory guide is being issued in draft form to involve the public in the early stages of the development of a regulatory position in this area. It has not received complete staff review and does not represent an official NRC staff position.

Public comments are being solicited on the draft guide (including any implementation schedule) and its associated regulatory analysis or value/impact statement. Comments should be accompanied by appropriate supporting data. Written comments may be submitted to the Rules Review and Directives Branch, DFIPS, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555. Copies of comments received may be examined at the NRC Public Document Room, 2120 L Street NW., Washington, DC. Comments will be most helpful if received by

Requests for single copies of draft or active regulatory guides (which may be reproduced) or for placement on an automatic distribution list for single copies of future draft guides in specific divisions should be made in writing to the U.S. Nuclear Regulatory Commission, Washington, DC 20555, Attention: Distribution and Mail Services Section, or by fax to (301)415-2260.

FOREWORD

The NRC's Policy Statement (Ref. 1) on probabilistic risk analysis (PRA) encourages greater use of this analysis technique to improve safety decisionmaking and improve regulatory efficiency. The NRC staff's PRA Implementation Plan describes activities now underway or planned to expand this use. These activities include, for example, providing guidance for NRC inspectors on focusing inspection resources on risk-important equipment, as well as reassessing plants with relatively high core damage frequencies for possible backfits.

Another activity under way in response to the policy statement is the use of PRA in support of decisions to modify an individual plant's current licensing basis (CLB). This regulatory guide provides guidance on the use of PRA findings and risk insights in support of licensee requests for changes to a plant's current licensing basis (e.g., request for license amendments and technical specification changes under 10 CFR §§50.90-92. It does not address licensee-initiated changes to the current licensing basis which do NOT require NRC review and approval (e.g., changes to the facility as described in the FSAR which are the subject of 10 CFR §50.59). Licensee-initiated CLB changes which are consistent with currently-approved Staff positions, e.g., regulatory guides, standard review plans, branch technical positions, or the Standard Technical Specifications, are normally evaluated by the staff using traditional, deterministic engineering analyses. A licensee would not be expected to submit risk information in support of the proposed change. Licensee-initiated CLB changes which request changes which go beyond current Staff positions may be evaluated by the Staff using traditional deterministic engineering analyses as well as the risk-informed approach set forth in this regulatory guide. A licensee may be requested to submit supplemental risk information or deterministic information if such information is not submitted by the licensee. If risk information on the proposed CLB change is not provided to the Staff, the Staff will review the information provided by the licensee to determine if the application can be approved based upon the information provided using traditional deterministic methods and will either approve or reject the application based upon the Staff's review. For those licensee-initiated CLB changes which a licensee chooses to support (or is requested by the staff to support) with risk information, this regulatory guide describes an acceptable method for assessing the nature and impact of proposed CLB changes by considering engineering issues and applying risk insights. Licensees submitting risk information (whether on their own initiative or at the request of the staff) should address each of the principles of risk-informed regulation discussed in this regulatory guide. Licensees should identify how chosen approaches and methods (whether they are quantitative or qualitative, and deterministic or probabilistic), data, and criteria for considering risk are appropriate for the decision to be made.

Finally, the guidance provided here does not preclude other approaches for requesting changes to the CLB. Rather, this Regulatory Guide is intended to improve consistency in regulatory decisions in areas in which the results of risk analyses are used to help justify regulatory action. As such, the principles, process, and approach discussed herein also provide useful guidance for the application of risk information to a broader set of activities than plant-specific changes to a plant's CLB (i.e., generic activities) and licensees are encouraged to utilize this guidance in that regard.

CONTENTS

| FOREWORD | <u>PAGE</u> ii |
|--|-------------------|
| 1. INTRODUCTION | 1-1 |
| 1.1 Background | 1-1 |
| 1.2 Purpose of the Regulatory Guide | 1-2 |
| 1.3 Scope of this Regulatory Guide | 1-2 |
| 1.4 Relationship to other Guidance Documents | 1-3 |
| 2. AN ACCEPTABLE APPROACH TO RISK-INFORMED DECISIONMAKING | 2-1 |
| 2.1 Risk-Informed Philosophy | 2-1 |
| 2.2 A Four-Element Approach to Integrated Decisionmaking | 2-3 |
| 2.3 Element 1: Define the Proposed change | 2-4 |
| 2.4 Element 2: Perform Engineering Analysis | 2-5 |
| 2.4.1 Evaluation of defense-in-Depth Attributes & Safety Margins | 2-5 |
| 2.4.1.1 Defense-in-Depth | 2-6 |
| 2.4.1.2 Safety Margins | 2-7 |
| 2.4.2 Evaluation of Risk Impact, Including Treatment of Uncertainties | 2-7 |
| 2.4.2.1 Acceptance Guidelines | 2-8 |
| 2.4.2.2 Comparison of PRA Results with the Acceptance Guidelines | 2-10 |
| 2.4.3 Integrated Decision-Making | 2-13 |
| 2.5 Element 3: Define Implementation and Monitoring Program | 2-14 |
| 2.6 Element 4: Submit Proposed Change | 2-16 |
| 2.7 Quality Assurance | 2-16 |
| 3. DOCUMENTATION AND SUBMITTAL | 3-1 |
| 3.1 Introduction | 3-1 |
| 3.2 Documentation | 3-1 |
| 3.3 Licensee Submittal | 3-1 |
| 3.4 Implementation Plan and Performance Monitoring Process | 3-4 |
| APPENDIX A. USE OF RISK IMPORTANCE MEASURES TO CATEGORIZE STRUCTURES, SYSTEMS, AND COMPONENTS WITH RESPECT TO SAFETY SIGNIFICANCE | A-1 |
| APPENDIX B. AN APPROACH ESTIMATING THE FREQUENCIES OF VARIOUS CONTAINMENT FAILURE MODES AND BYPASS EVENTS | B-1 |
| B.1 INTRODUCTION | B-1 |
| B.2 PWRs with Large Volume Containments | B-1 |
| B.3 PWRs Ice Condenser Containments | B-6 |
| B.4 BWR Mark I Containment | B-8 |
| B.5 BWR Mark II Containment | B-11 |
| B.6 BWR Mark III Containment | B-14 |
| ATTACHMENT TO APPENDIX B | |
| Definition of Containment Failure Mode Classes | B-18 |

1. INTRODUCTION

1.1 Background

During the last several years, both the NRC and the nuclear industry have recognized that probabilistic risk assessment (PRA) has evolved to the point where it can be used increasingly as a tool in regulatory decisionmaking. In August 1995, the NRC adopted the following policy statement regarding the expanded use of PRA.

- The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.
- PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices. Where appropriate, PRA should be used to support the proposal of additional regulatory requirements in accordance with 10 CFR 50.109 (Backfit Rule). Appropriate procedures for including PRA in the process for changing regulatory requirements should be developed and followed. It is, of course, understood that the intent of this policy is that existing rules and regulations shall be complied with unless these rules and regulations are revised.
- PRA evaluations in support of regulatory decisions should be as realistic as practicable and appropriate supporting data should be publicly available for review.
- The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgements on need for proposing and backfitting new generic requirements on nuclear power plant licensees.

In its approval of the policy statement, the Commission articulated its expectation that implementation of the policy statement will improve the regulatory process in three areas: foremost, through safety decisionmaking enhanced by the use of PRA insights; through more efficient use of agency resources; and through a reduction in unnecessary burdens on licensees.

In parallel with the publication of the policy statement, the staff developed an implementation plan to define and organize the PRA-related activities being undertaken. These activities cover a wide range of PRA applications and involve the use of a variety of PRA methods (with variety including both types of models used and the detail of modeling needed). For example, one application involves the use of PRA in the assessment of operational events in reactors. The characteristics of these assessments permit relatively simple PRA models to be used. In contrast, other applications require the use of detailed models.

The activities described in the PRA Implementation Plan relate to a number of agency interactions with the regulated industry. With respect to reactor regulation, activities include, for example, guidance development for NRC inspectors on focusing inspection resources on risk-important equipment, and a reassessment of plants with relatively high core damage frequencies for possible backfit.

Introduction

This regulatory guide focuses on the use of PRA in a subset of the applications described in the staff's implementation plan. Its principal focus, and that of the supporting staff document (draft NUREG-1602, Ref. 2), is the use of PRA findings and risk insights in decisions on proposed changes to a plant's current licensing basis (CLB).¹ Such CLB changes are expected to result in improved reactor safety by incorporating advances in technology and lessons learned from operating experience, or fixing vulnerabilities identified through analysis or other means and, in addition, may result in the removal of unnecessarily burdensome regulatory practices.

The regulatory guide also makes use of the Commission's Safety Goal Policy Statement. As discussed below, one key principle in risk-informed regulation is that increases in risk be small and do not cause the NRC Safety Goals to be exceeded. The Commission's Safety Goals (and associated quantitative health objectives (QHOs)) define an acceptable level of risk which is a small fraction (0.1%) of other risks to which the public is exposed. The acceptance guidelines defined in this regulatory guide (in Section 2.4.2) are based on subsidiary objectives derived from the Safety Goals and their QHOs.

1.2 Purpose of the Regulatory Guide

Changes to many of the activities and design characteristics in a nuclear power plant's current licensing basis require NRC review and approval. This regulatory guide provides the Staff's recommendations for utilizing risk information in support of licensee-initiated CLB changes requiring such review and approval. The guidance provided here does not preclude other approaches for requesting CLB changes. Rather, this regulatory guide is intended to improve consistency in regulatory decisions in areas in which the results of risk analyses are used to help justify regulatory action. As such, this regulatory guide, the use of which is voluntary, provides general guidance concerning one approach that the NRC has determined to be acceptable for analyzing issues associated with proposed changes to a plant's current licensing basis (CLB) and for assessing the impact of such proposed changes on the risk associated with plant design and operation. This guidance does not address the specific analyses needed for each nuclear power plant activity or design characteristic that may be amenable to risk-informed regulation.

1.3 Scope of this Regulatory Guide

This regulatory guide describes an acceptable approach for assessing the nature and impact of proposed CLB changes by considering engineering issues and applying risk insights. Assessments should consider relevant safety margins and defense-in-depth attributes, including consideration of success criteria as well as equipment functionality, reliability, and availability. The analyses should reflect the actual design, construction, and operational practices of the plant. Acceptance guidelines for evaluating the results of such assessments are provided also. This guide also addresses implementation strategies and performance monitoring plans associated with CLB changes that will help ensure assumptions and analyses supporting the change are verified.

¹This regulatory guide adopts the 10 CFR Part 54 definition of current licensing basis. That is, "Current Licensing Basis (CLB) is the set of NRC requirements applicable to a specific plant and a licensee's written commitments for ensuring compliance with and operation with in applicable NRC requirements and the plant-specific design basis (including all modifications and additions to such commitments over the life of the license) that are docketed and in effect. The CLB includes the NRC regulations contained in 10 CFR Parts 2, 19, 20, 21, 26, 30, 40, 51, 54, 55, 70, 72, 73, 100 and appendices thereto; orders; license conditions; exemptions; and technical specifications. It also includes the plant-specific design-basis information defined in 10 CFR 50.2 as documented in the most recent final safety analysis report (FSAR) as required by 10 CFR 50.71 and the licensee's commitments remaining in effect that were made in docketed licensing correspondence such as licensee responses to NRC bulletins, generic letters, and enforcement actions, as well as licensee commitments documented in NRC safety evaluations or licensee event reports."

Consideration of the Commission's Safety Goal Policy Statement is an important element in regulatory decisionmaking. Consequently, this regulatory guide provides acceptance guidelines consistent with the Commission's Safety Goal Policy Statement.

In theory, one could construct a more generous regulatory framework for consideration of those risk-informed changes which may have the effect of increasing risk to the public. Such a framework would include, of course, assurance of continued adequate protection (that level of protection of the public health and safety which must be reasonably assured regardless of economic cost). But it could also include provision for possible elimination of all measures not needed for adequate protection which either do not effect a substantial reduction in overall risk or result in continuing costs which are not justified by the safety benefits. Instead NRC has chosen, in this regulatory guide, a more restrictive policy which would permit only small increases in risk, and then only when it is reasonably assured, among other things, that sufficient defense in depth and sufficient margins are maintained. This policy is adopted because of the inherent uncertainties in PRA and to account for the fact that safety issues continue to emerge regarding design, construction, and operational matters notwithstanding the maturity of the nuclear power industry. These factors suggest that nuclear power reactors should operate routinely only at a prudent margin above adequate protection. The safety goal subsidiary objectives are used as an example of such a prudent margin.

Finally, this regulatory guide indicates an acceptable level of documentation that will enable the staff to reach a finding that the licensee has performed a sufficiently complete and scrutable analysis and that the results of the engineering evaluations support the licensee's request for a regulatory change.

1.4 Relationship to Other Guidance Documents

Directly relevant to this regulatory guide is the Standard Review Plan (SRP) designed to guide the NRC staff evaluations of licensee requests for changes to the CLB that apply risk insights, as well as selected application-specific regulatory guides and the corresponding Standard Review Plan chapters. Related regulatory guides include DG-1062 (Ref. 3) on inservice testing, DG-1063 (Ref. 4) on inservice inspection of piping, DG-1064 (Ref. 5) on graded quality assurance, and DG-1065 (Ref. 6) on technical specifications. Draft NUREG-1602 contains reference material on issues and methods for PRA that can be used to support regulatory decisionmaking. The staff recognizes that the risk analyses necessary to support regulatory decisionmaking may vary with the relative weight that is given to the risk assessment element of the decisionmaking process. The burden is on the licensee requesting a change to their CLB to justify why the chosen risk assessment approach, methods, and data are appropriate for the decision to be made.

2. AN ACCEPTABLE APPROACH TO RISK-INFORMED DECISIONMAKING

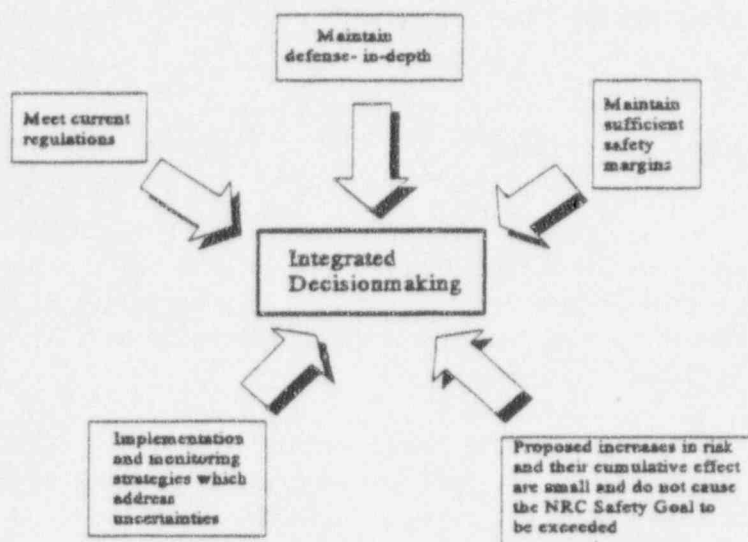
2.1 Risk-Informed Philosophy

In its approval of the policy statement on the use of PRA methods in nuclear regulatory activities, the Commission stated an expectation that "the use of PRA technology should be increased in all regulatory matters...in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy." The use of risk insights in licensee submittals requesting CLB changes will assist the staff in the disposition of such licensee proposals.

The staff has defined an acceptable approach to analyzing and evaluating proposed CLB changes. This approach supports the NRC's desire to base its decisions on the results of traditional engineering evaluations, supported by insights (derived from the use of PRA methods) about the risk significance of the proposed changes. Decisions concerning proposed changes are expected to be reached in an integrated fashion, considering traditional engineering and risk information, and may be based on qualitative factors as well as quantitative analyses and information.

In implementing risk-informed decisionmaking, changes are expected to meet a set of key principles. Some of these principles are written in terms typically used in traditional engineering decisions (e.g., defense-in-depth). While written in these terms, it should be understood that risk analyses techniques can be, and are encouraged to be, used to help ensure and show that they are met. These principles are:

1. The proposed change meets the current regulations. This principle applies unless the proposed change is explicitly related to a requested exemption or rule change (i.e., a 50.12 "specific exemption" or a 2.802 "petition for rulemaking").
2. Defense-in-depth is maintained.
3. Sufficient safety margins are maintained.
4. Proposed increases in risk, and their cumulative effect, are small and do not cause the NRC Safety Goals to be exceeded.
5. Performance-based implementation and monitoring strategies are proposed that address uncertainties in analysis models and data and provide for timely feedback and corrective action.



Each of these principles should be considered in the risk-informed, integrated decisionmaking process, as illustrated in Figure 1 below.

Figure 1. Principles of Risk-Informed Regulation

The staff's proposed evaluation approach and acceptance guidelines follow from these principles. In implementing these principles, the staff expects that:

- All safety impacts of the proposed change are evaluated in an integrated manner as part of an overall risk management approach in which the licensee is using risk analysis to improve operational and engineering decisions broadly and not just to eliminate requirements the licensee sees as undesirable. The approach used to identify changes in requirements should be used to identify areas where requirements should be increased,¹ as well as where they could be reduced.

¹ The staff is aware of, but does not endorse here, guidelines which have been developed (e.g., by NEI/NUMARC in NUMARC 91-04) (Ref. 7) to assist in identifying potentially beneficial changes to requirements.

- The acceptability of proposed changes should be evaluated by the licensee in an integrated fashion that ensures that all principles are met.²
- Core damage frequency (CDF) and large early release frequency (LERF)³ can be used as suitable metrics for making risk-informed regulatory decisions.
- Increases in estimated CDF and LERF resulting from proposed CLB changes will be limited to small increments.
- The scope and quality of the engineering analyses (including traditional and probabilistic analyses) conducted to justify the proposed CLB change should be appropriate for the nature and scope of the change and should be based on the as-built and as-operated and maintained plant.⁴
- Appropriate consideration of uncertainty is given in analyses and interpretation of findings.
- The plant-specific PRA supporting licensee proposals has been subjected to quality controls such as an independent peer review.⁵
- Data, methods, and assessment criteria used to support regulatory decisionmaking must be scrutable and available for public review.

2.2 A Four-Element Approach to Integrated Decisionmaking

Given the principles of risk-informed decisionmaking discussed above, the staff has identified a four-element approach to evaluating proposed CLB changes. This approach, which is presented graphically in Figure 2, acceptably supports the NRC's decisionmaking process. This approach is not sequential in nature; rather it is iterative.

² One important element of integrated decisionmaking can be the use of an "expert panel." Such a panel is not a necessary component of risk-informed decisionmaking; but when it is used, the key principles and associated decision criteria presented in this regulatory guide still apply and must be shown to have been met or to be irrelevant to the issue at hand.

³ In this context, LERF is being used as a surrogate for the early fatality QHO. It is defined as the frequency of those accidents leading to significant, unmitigated releases from containment in a time frame prior to effective evacuation of the close-in population such that there is a potential for early health effects. Such accidents generally include unscrubbed releases associated with early containment failure at or shortly after vessel breach, containment bypass events, and loss of containment isolation. This definition is consistent with accident analysis used in the safety goal screening criteria discussed in the Commission's Regulatory Analysis Guidelines.

⁴ Draft NUREG-1602 provides supplemental information on PRA attributes.

⁵ As discussed in Section 2.4.2 below, such a peer review is not a replacement for NRC review.

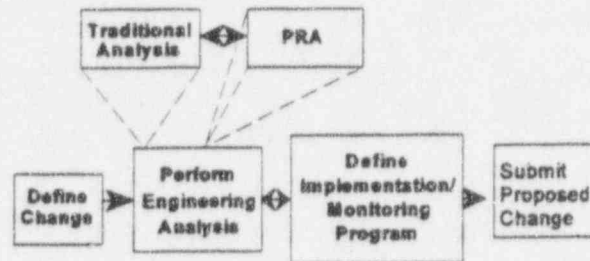


Figure 2. Principal Elements of Risk-Informed, Plant-Specific Decisionmaking

2.3 Element 1: Define the Proposed Change

Element 1 involves three primary activities. First, the licensee should identify those aspects of the plant's licensing bases that may be affected by the proposed change, including, but not limited to, rules and regulations, final safety analysis report (FSAR), technical specifications, licensing conditions, and licensing commitments. Second, the licensee should identify all SSCs, procedures, and activities that are covered by the CLB change under evaluation and consider the original reasons for inclusion of each program requirement.

When considering CLB changes, a licensee may identify regulatory requirements or commitments in its licensing bases that it believes are overly restrictive or unnecessary to ensure safety at its plant. Note that the corollary is also true; that is, licensees are expected also to identify possible cases where design and operational aspects of the plant should be enhanced consistent with an improved understanding of their safety significance. Such enhancements should be embodied in appropriate CLB changes which reflect these enhancements. With this staff expectation in mind, the licensee should, third, identify available engineering studies, methods, codes, applicable plant-specific and industry data and operational experience, PRA findings, and research and analysis results relevant to the proposed CLB change. With particular regard to the plant-specific PRA, the licensee should assess the capability to use, refine, augment, and update system models as needed to support a risk assessment of the proposed CLB change.

The above information should be used collectively to provide a description of the CLB change and to outline the method of analysis. The licensee should describe the proposed change and how it meets the objectives of the Commission's PRA Policy Statement, including enhanced decisionmaking, more efficient use of resources, and reduction of unnecessary burden. In addition to improvements in reactor safety, this assessment may consider benefits from the CLB change such as reduced fiscal and personnel resources and radiation exposure. In addition, the licensee should affirm that the proposed CLB change meets the current

regulations, unless the proposed change is explicitly related to a proposed exemption or rule change (i.e., a 50.12 "specific exemption" or a 2.802 "petition for rulemaking").

2.4 Element 2: Perform Engineering Analysis

As part of the second element, the licensee will evaluate the proposed CLB change with regard to the principles that adequate defense-in-depth is maintained, that sufficient safety margins are maintained, and that proposed increases in risk, and their cumulative effect, are small and do not cause the NRC Safety Goals to be exceeded.

The staff expects that the scope and quality of the engineering analyses conducted to justify the proposed CLB change will be appropriate for the nature and scope of the change. The staff also expects that appropriate consideration will be given to uncertainty in the analysis and interpretation of findings. The licensee is expected to use its judgment, drawing from the appropriate technical disciplines for the CLB change being considered, of the complexity and difficulty of implications of the proposed CLB change to decide upon adequate engineering analyses to support regulatory decisionmaking. Thus, the licensee should consider the appropriateness of qualitative and quantitative analyses, as well as analyses using traditional engineering approaches and those techniques associated with the use of PRA findings. Regardless of the analysis methods chosen, the licensee must show that the principles set forth in Section 2.1 have been met through the use of scrutable acceptance guidelines established for making that determination.

Some proposed CLB changes can be characterized as involving the categorization of SSCs according to safety significance. An example is grading the application of quality assurance controls commensurate with the safety significance of equipment. The licensee's analyses of the impact of the proposed CLB change should address each of the key principles of risk-informed regulation (discussed previously in Section 2.1 of this regulatory guide). Like other applications, the staff's review of CLB change requests for applications involving safety categorization will be according to the acceptance guidelines which are associated with each key principle and which are presented in this regulatory guide (see Sections 2.4.1, 2.4.2, and 2.5), unless equivalent guidelines are proposed by the licensee. Since risk importance measures are often used in such categorizations, guidance on their use is provided in Appendix A of this regulatory guide. For such CLB changes, guidelines associated with the adequacy of programs (in this example, quality controls) implemented for different safety significant categories (e.g., more safety significant and less safety significant) are addressed in other application-specific regulations and guidance documents. Licensees are encouraged to apply risk-informed findings and insights to decisions (and potential CLB requests) associated with what are appropriate, for instance, test methods, surveillance intervals, or quality controls.

2.4.1 Evaluation of Defense-in-Depth Attributes & Safety Margins

One aspect of the engineering evaluations is to show that the fundamental safety principles on which the plant design was based are not compromised. Design basis accidents (DBAs) play a central role in nuclear power plant design. DBAs are a combination of postulated challenges and failure events against which plants are designed to ensure adequate and safe plant response. During the design process, plant response and associated safety margins are evaluated using assumptions which are intended to be conservative.

Draft for Comment

Acceptable Approach

National standards and other considerations such as defense-in-depth attributes and the single failure criterion constitute additional engineering considerations that influence plant design and operation. Margins and defenses associated with these considerations may be affected by the licensee's proposed CLB change and, therefore, should be reevaluated to support a requested CLB change. As part of this evaluation, the impact of the proposed CLB change on affected equipment functionality, reliability, and availability should be determined.

2.4.1.1 Defense-in-Depth

The engineering evaluation conducted should evaluate whether the impact of the proposed CLB change (individually and cumulatively) is consistent with the principle that defense-in-depth is maintained. In this regard, the intent of the principle is to assure that the philosophy of defense-in-depth is maintained, not to prevent changes in the way defense-in-depth is achieved. The defense-in-depth philosophy has traditionally been applied in reactor design and operation to provide multiple means to accomplish safety functions and prevent the release of radioactive material. It has been and continues to be an effective way to account for uncertainties in equipment and human performance. Where a comprehensive risk analysis can be done, it can be used to help determine the appropriate extent of defense-in-depth (e.g., balance among core damage prevention, containment failure and consequence mitigation) to ensure protection of public health and safety. Where a comprehensive risk analysis is not or cannot be done, traditional defense-in-depth considerations should be used or maintained to account for uncertainties. The evaluation should consider the intent of the general design criteria, national standards, and engineering principles such as the single failure criterion. Further, the evaluation should consider the impact of the proposed CLB change on barriers (both preventive and mitigative) to core damage, containment failure or bypass, and the balance among defense-in-depth attributes. As stated earlier, the licensee should select the engineering analysis techniques, whether quantitative or qualitative and traditional or probabilistic, appropriate to the proposed CLB change.

The licensee should assess whether the proposed CLB change meets the defense-in-depth principle. Defense-in-depth consists of a number of elements, as summarized below. These elements can be used as guidelines for making that assessment. Other equivalent acceptance guidelines may also be used.

- Defense-in-depth is maintained
 - a reasonable balance among prevention of core damage, prevention of containment failure, and consequence mitigation is preserved
 - over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided
 - system redundancy, independence, and diversity are preserved commensurate with the expected frequency and consequences of challenges to the system (e.g., no risk outliers)
 - defenses against potential common cause failures are preserved and the potential for introduction of new common cause failure mechanisms is assessed

- independence of barriers is not degraded
- defenses against human errors are preserved

2.4.1.2 Safety Margins

The engineering evaluation conducted should assess whether the impact of the proposed CLB change is consistent with the principle that sufficient safety margins are maintained. Here also, the licensee is expected to choose the method of engineering analysis appropriate for evaluating whether sufficient safety margins would be maintained if the proposed CLB change were implemented. An acceptable set of guidelines for making that assessment are summarized below. Other equivalent acceptance guidelines may also be used.

- Sufficient safety margins are maintained
 - codes and standards or alternatives approved for use by the NRC are met
 - safety analysis acceptance criteria in the current licensing basis (e.g., FSAR, supporting analyses) are met, or proposed revisions provide sufficient margin to account for analysis and data uncertainty

Application-specific guidelines reflecting this general guidance may be found in the application-specific regulatory guides.

2.4.2 Evaluation of Risk Impact, Including Treatment of Uncertainties

As noted in Section 2.1, the licensee's risk assessment should be used to address the principle that proposed increases in risk, and their cumulative effect, are small and do not cause the NRC Safety Goals to be exceeded. For purposes of implementation, the licensee should assess the expected change in core damage frequency (CDF) and large early release frequency (LERF). The necessary sophistication of the evaluation, including the scope of the PRA (e.g., internal events only, full power only), depends on the contribution the risk assessment makes to the integrated decision-making, which depends to some extent on the magnitude of the potential risk impact. For some CLB changes for which a more substantial impact is possible, an in-depth and comprehensive PRA analysis of appropriate scope to derive a quantified estimate of the total impact of a proposed CLB change will be necessary to provide adequate justification. In other applications, calculated risk importance measures or bounding estimates will be adequate. In still others, a qualitative assessment of the impact of the CLB change on the plant's risk may be sufficient.

The PRA performed should realistically reflect the actual design, construction, and operational practices. Consequently, the PRA used to support risk-informed decisionmaking is expected to reflect the impact of previous changes made to the CLB.

The remainder of this section discusses the use of quantitative PRA results in decisionmaking. One of the strengths of the PRA framework is its ability to provide a means of characterizing the impact of analytical uncertainty, and it is essential that these uncertainties be recognized when assessing whether the principles

are being met. To provide a vehicle for consistency between submittals and the review of those submittals, the following guidelines on how to address uncertainty in the decisionmaking process are provided. The first step is the definition of a set of quantitative acceptance guidelines. Second, the role of uncertainty analysis in decisionmaking is discussed. The staff's decision on the proposed license amendment will be based on its independent judgment and review, as appropriate, of the entire application.

2.4.2.1 Acceptance Guidelines

The risk acceptance guidelines presented in this regulatory guide are based on the principles and expectations for risk-informed regulation discussed in Section 2.1. For the purposes of establishing guidelines for risk-informed decisionmaking, a core damage frequency (CDF) guideline of 1E-4 per reactor year (annual average of CDF) has been adopted in this regulatory guide. (with additional management attention for the 1E-5 to 1E-4 per reactor year range). A large early release frequency (LERF) of 1E-5 per reactor year (annual average of LERF) has been adopted as a containment performance guideline. (with additional management attention for the 1E-5 to 1E-6 per reactor year range). These guidelines are intended for comparison with a full scope PRA (including internal events, external events, full power, low power and shutdown). However, it is recognized that many PRAs are not full scope and the use of less than full scope PRA information may be acceptable as discussed in Section 2.4.2.2 of this regulatory guide.

The acceptance guidelines have the following elements:

- For a plant with a mean core damage frequency at or above 1E-4 per reactor year (the Commission's subsidiary core damage frequency objective) or with a mean LERF at or above 1E-5 per reactor year, it is expected that applications will result in a net decrease in risk or be risk neutral.
- For a plant with a mean core damage frequency of less than 1E-4 per reactor year, applications will be considered which, when combined with the LERF guidelines described below:
 - Result in a net decrease in CDF or are CDF-neutral;
 - Result in increases in calculated CDF that are very small (e.g., CDF increase of less than 1E-6 per reactor year); or
 - Result in an increase in calculated CDF in the range of 1E-6 to 1E-5 per reactor year, subject to increased NRC technical and management review and considering the following factors:
 - The scope, quality, and robustness of the analysis (including, but not limited to, the PRA), including consideration and quantification of uncertainties;
 - The base CDF and LERF of the plant;
 - The cumulative impact of previous changes (the licensee's risk management approach);
 - Consideration of the Safety Goal screening criteria in the staff's Regulatory Analysis Guidelines, which define what changes in CDF and containment performance would be needed to consider potential backfits;

- The impact of the proposed change on operational complexity, burden on the operating staff, and overall safety practices; and
- Plant-specific performance and other factors, including, for example, siting factors, inspection findings, performance indicators, and operational events.

AND

- For a plant with a mean LERF of between $1\text{E-}6$ and $1\text{E-}5$ per reactor year:
 - Result in a net decrease in LERF or are LERF-neutral;
 - Result in an increase in calculated LERF of up to $1\text{E-}5$ per reactor year, subject to increased NRC technical and management review, as described above;

OR

- For a plant with a mean LERF of less than $1\text{E-}6$ per reactor year:
 - Result in a net decrease in LERF or are LERF-neutral;
 - Result in increases in calculated LERF that are very small (e.g., LERF increase of less than $1\text{E-}7$ per reactor year); or
 - Result in an increase in calculated LERF of up to $1\text{E-}6$ per reactor year, subject to increased NRC technical and management review, as described above.

The rigor of analyses needed to support the different types of applications is discussed in Section 2.4.2.2 below.

2.4.2.2 Comparison of PRA Results with the Acceptance Guidelines

In comparing estimates of plant risk (i.e., calculated plant CDF and LERF) and changes in these metrics as a result of CLB changes with the acceptance guidelines, it is necessary to take into account the uncertainties in the analysis. This section provides guidance on the comparison of the PRA results with the acceptance guidelines with particular reference to the role of uncertainty analysis.

Types of Uncertainty and Methods of Analysis

Because they are generally characterized and treated differently, it is useful to identify three classes of uncertainty: parameter uncertainty, model uncertainty, and completeness uncertainty.

Parameter Uncertainty Parameter uncertainties are those associated with the values of the fundamental parameters of the PRA model, such as equipment failure rates, initiating event frequencies, and human error probabilities that are used in the quantification of the accident sequence frequencies. They are typically characterized by establishing probability distributions on the parameter values. It is straightforward and within the capability of most PRA codes to propagate the distribution representing uncertainty on the basic

Draft for Comment

Acceptable Approach

parameter values to generate a probability distribution on the results (CDF, accident sequence frequencies, etc.) of the PRA. This is in fact the only practical way of generating a mean value of the CDF. However, the analysis must be done carefully to correlate the sample values for different components from a group to which the same parameter value applies (the so-called state of knowledge dependency).

Parameter uncertainties can be explicitly represented and propagated through the PRA model, and the probability distribution of the relevant metrics (i.e., CDF and Δ CDF, and LERF and Δ LERF) can be generated. Various measures of central tendency, such as the mean, median and mode, can be evaluated. In principle, the distributions can be used to assess the confidence with which the guidelines are met. However, it is also instructive to study the contributors to see whether it can be determined whether the tails of the distributions are being determined by uncertainties on a few significant elements of the model. If so, these elements can be identified as candidates for compensatory measures and/or monitoring during integrated decisionmaking.

Model Uncertainty There are also uncertainties as to how to model certain elements of the PRA. Model uncertainty may be analyzed in different ways. It is possible to include some model uncertainty by incorporating within the PRA model a discrete probability distribution over a set of models for a particular issue. This has been done for the modeling of seismic hazard, for example, where the result is a discrete probability distribution on the frequencies of earthquakes. This uncertainty can then be propagated in the same way as the parameter uncertainties. Other methods are also available. For most Level 1 PRAs, there are few model uncertainties explicitly represented in the model structure. Instead, where it is necessary to address issues that are uncertain, e.g., success criteria, it is more usual for the analysts to adopt a specific assumption or modeling approach. Thus the effect of model uncertainties is generally to introduce some type of bias into the results.

There are significant model uncertainties in Level 2 PRAs, particularly in the modeling of the phenomenology of accident progression and the mechanisms for the release of fission products. Again, some uncertainties are addressed by making specific assumptions. However, others may be incorporated in the level 2 analysis by, for example, including within the structure of the containment event trees a set of possible outcomes for the uncertain issues. NUREG-1150 (Ref. 8) provides examples of an attempt to characterize the full impact of the uncertainty. In many PRAs, however, the conditional containment probabilities or large early release fractions represent an average over these outcomes.

It is often instructive to understand the impact of a specific assumption on the predictions of the model. The impact of using alternate assumptions or models may be addressed by performing appropriate sensitivity studies, or they may be addressed using qualitative arguments.

Completeness Uncertainty Completeness is not in itself an uncertainty, but a reflection of scope limitations. The result is, however, an uncertainty about where the true risk lies. The problem with completeness uncertainty is that, because it reflects an unanalyzed contribution, it is difficult (if not impossible) to estimate its magnitude. Thus, for example, the impact on actual plant risk from unanalyzed issues such as the influences of organizational performance cannot now be explicitly assessed.

The issue of completeness of scope of a PRA can be addressed by either supplementing the analysis with additional analysis to enlarge the scope, using more restrictive acceptance guidelines, or by providing arguments that, for the application of concern, the out-of-scope contributors are not significant. Acceptable approaches to dealing with incompleteness are discussed in the next section.

Comparisons with Acceptance Guidelines

The purpose of this section is to provide guidance on how to compare the results of the PRA with the acceptance guidelines described in Section 2.4.2.1. In the context of decisionmaking, the acceptance guidelines should not be interpreted as being overly prescriptive. They are intended to provide an indication, in numerical terms, of what is considered acceptable. As such, the numerical guidelines described in this regulatory guide are approximate values that provide an indication of the changes that are generally acceptable. Furthermore, the epistemic uncertainties associated with PRA calculations preclude a definitive decision of acceptability or unacceptability based purely on the numerical results. The intent in making the comparison of the PRA results with the acceptance guidelines is to demonstrate with reasonable assurance that Principle 4, discussed in Section 2.1, is being met. This decision must be made based on a full understanding of the impacts of the uncertainties, both those that are explicitly accounted for in the results and those that are not. This is a somewhat subjective process, and the reasoning behind the decisions must be well documented.

The three types of uncertainty can be addressed as follows to demonstrate reasonable assurance: 1) those uncertainties that are explicitly quantified in the model (parameter uncertainties and some model uncertainties) do not produce a probability distribution on the estimated value of CDF or LERF that results in a low level of confidence that the goal is met; 2) the adoption of specific modeling does not overly bias the results in favor of the change and alternate, but reasonable, modeling assumptions would not alter the decision (model uncertainty); and, 3) the contributors to risk that are not modeled would not alter the decision significantly (completeness uncertainty). The discussion presented here addresses quantitative analyses of uncertainties; qualitative arguments may be appropriate for specific CLB changes.

The level of detail required in the analysis of uncertainty will depend on the CLB change being considered, the base case estimates of CDF or LERF, and the potential impact of the change on those metrics. The closer the base case estimates and the estimates of the impact of the change are to their corresponding acceptance guidelines, the more detail will be required. In contrast, if, as an example, the estimated change in a particular metric is very small compared to the acceptance goal, a simple bounding analysis or even a qualitative analysis may suffice.

Changes resulting in a net decrease in the CDF and LERF estimates are allowed irrespective of the calculated baseline CDF and LERF. Generally, it should be possible to argue on the basis of an understanding of the contributors and the changes that are being made that the overall impact is indeed a decrease, without the need for a detailed uncertainty analysis.

In the initial comparison of the PRA results to the acceptance guidelines, the appropriate numerical measures to use are mean values. In general, if the change is such that it would result in either the point estimate or mean value of the CDF or LERF or the corresponding increase (Δ CDF or Δ LERF) exceeding its guideline,

Draft for Comment

Acceptable Approach

the change will not be approved unless, for example, it is shown that there are unquantified benefits that are not reflected in the quantitative risk results. In addition, if convincing qualitative arguments are made that the analysis is conservative, or compensatory measures are proposed to counter the impact of the major risk contributors, even though the impact of these measures may not be estimated numerically, then such arguments will be considered in the decision process. Finally, changes which result in very small increases in the estimates of CDF or LERF might be allowable even for plants for which the base case approaches the guidelines, but again, only if additional qualitative arguments can be made as discussed above.

If the mean value of a measure were to lie near the corresponding guideline a full parametric, uncertainty analysis will allow an assessment of the confidence with which the guideline is met. Because of the nature of PRA analyses, it is not reasonable to be so prescriptive about the acceptable level of confidence; changes could still be allowed when lower levels of confidence are calculated when, as discussed above, convincing qualitative arguments that the true values are less than the calculated values can be brought to bear. Such arguments can only be made with a full understanding of the contributors to uncertainty.

While the analysis of parametric uncertainty is fairly mature, the analysis of the model and completeness uncertainties cannot be handled in such a formal manner. Whether the PRA is full scope or only partial scope, it will be incumbent on the licensee to demonstrate that the choice of reasonable alternate hypotheses or modeling approximations or methods to those adopted in the PRA model would not significantly change the assessment. The alternates that would drive the result towards unacceptability should be identified and reasons given as to why they are not appropriate for the current application or for the particular plant. Alternatively, this analysis can be used to identify candidates for compensatory actions or increased monitoring. The licensee should concentrate its attention on those assumptions which impact the parts of the model being exercised by the change.

When the PRA is not full scope, then it is necessary for the licensee to address the significance of the out-of-scope items. The importance of assessing the contribution of the out-of-scope portions of the PRA to the base case estimates of CDF and LERF is related to the margin between the as-calculated values and the acceptance guidelines. When the contributions from the modeled contributors are close to the guidelines, the argument that the contribution from the missing items is not significant must be convincing, and in some cases may require additional PRA analyses. When the margin is significant, a qualitative argument may be sufficient. The contribution of the out-of-scope portions of the model to the change in metric may be addressed by bounding analyses, detailed analyses, or by a demonstration that the change has no impact on the unmodeled contributors. In addition, it should also be demonstrated that changes based on a partial PRA do not disproportionately change the risk associated with those accident sequences that arise from the modes of operation not included in the PRA.

If just a level 1 PRA is available, in general only the CDF is calculated and not the LERF. An approach is presented in Appendix B to this regulatory guide which allows a subset of the core damage accidents identified in the Level 1 analysis to be allocated to a release category that is equivalent to a LERF. The approach uses simplified event trees that can be quantified by the licensee on the basis of the plant configuration applicable to each accident sequence in the Level 1 analysis. The frequency derived from these event trees can be compared to the LERF acceptance guidelines. The guidance in Appendix B may

be used to estimate LERF in only those cases when the plant is not close to the CDF and LERF benchmark values.

2.4.3 Integrated Decision-Making

The results of the different elements of the engineering analysis discussed in Sections 2.4.1 and 2.4.2 must be considered in an integrated manner. None of the individual analyses is sufficient in and of itself. In this way, it can be seen that the decision is not driven solely by the numerical results of the PRA. They are one input into the decisionmaking and help in building up an overall picture of the implications of the proposed change on risk. The PRA has an important role in putting the change into its proper context as it impacts the plant as a whole.

2.5 Element 3: Define Implementation and Monitoring Program

Careful consideration should be given to implementation and performance-monitoring strategies. The primary goal for this element is to assess SSC performance under the proposed CLB change by establishing performance-monitoring strategies to confirm the assumptions and analyses that were conducted to justify the CLB change.

The implementation of the regulatory changes should ensure that no unexpected adverse safety degradation occurs because of the changes. Based on the findings of the engineering evaluations conducted to examine the impact of the proposed changes, an implementation plan should be developed to ensure that any unexpected problems and deficiencies are detected and corrected prior to becoming a significant safety problem. Further details of an acceptable process for implementation in specific application areas are discussed in the application-specific guides.

Decisions concerning implementation of changes should be made in light of the uncertainty associated with the results of the traditional 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, engineering evaluations are verified and validated, etc.), whereas a slower, phased approach to implementation (or other modes of partial implementation) would be expected when uncertainty in evaluation findings is higher. In applications where programmatic changes are being made which potentially impact SSCs across a wide spectrum of the plant, such as in IST, ISI and graded QA, the potential introduction of common cause effects must be fully considered and included in the submittal. In such situations, a carefully planned approach to the selected mode of implementation should be identified and justified.

A monitoring program, utilizing appropriate performance-based feedback criteria, is an important element of many risk informed application approaches. This performance-based approach should have the following attributes: there are measurable parameters to monitor plant performance; objective criteria are established to assess performance based on a combination of risk insights, traditional engineering analysis, and performance history; and parameters are selected for monitoring such that, if exceeded, they will provide early indication of problems prior to being a safety concern.

Draft for Comment

Acceptable Approach

Specifically, the proposed monitoring program should establish a means to adequately track the performance of equipment covered by the proposed licensing changes. The program should be capable of trending equipment performance after a change has been implemented to demonstrate that performance is consistent with that predicted by the traditional engineering and probabilistic analyses that were conducted to justify the change. It is desirable that definitive and quantitative performance criteria be established which are consistent with analysis assumptions and expectations in such areas as SSC functionality and reliability/availability. The monitoring plan should be structured such that performance degradation is detected and corrected before plant safety can be compromised. The potential impact of observed SSC degradation on similar components in different systems throughout the plant should be considered.

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. In these cases, the performance criteria chosen should be shown to be appropriate for the application in question. It should be noted that plant or licensee performance under actual design conditions may not be readily measurable. In cases where actual conditions cannot be monitored or measured, an approach should be implemented by striving to use whatever information most closely approximates actual performance data. For example, a hierarchy for establishing a monitoring program with a performance based-feedback approach may consist of a combination of the following:

1. Monitoring performance characteristics under actual design bases conditions (e.g., reviewing actual demands on EDGs, reviewing operating experience)
2. Monitoring performance characteristics under test conditions that are similar to those expected during a design basis event (e.g., monthly EDG testing)
3. Monitoring and trending performance characteristics to verify aspects of the underlying analysis, research, or bases for a requirement (e.g., measuring battery voltage and specific gravity, inservice inspection of piping)
4. Evaluating licensee performance during training scenarios (e.g., emergency planning exercises, operator licensing examinations)
5. Component quality controls including developing pre- and post- component installation evaluations (e.g., environmental qualification inspections, RPS channel checks, continuity testing of BWR squib valves)
6. Establishing performance-based elements (e.g., monitoring, measurement) where actual performance-based measurements may be impractical (i.e., performance-based elements of a QA program observing activities vs. reviewing programs)

As part of the monitoring program, it is important that provisions for specific cause determination and corrective actions be included in cases when performance falls below expected levels. Cause determination is needed when a performance criteria is not being met or when there is a functional failure of an application-specific SSC, even if performance criteria is met. The cause determination should identify the cause of the

failure or degraded performance, and whether the failure or degraded performance was a result of the application. It should address failure significance, the circumstances surrounding the failure or degraded performance, the characteristics of the failure, and whether the failure is isolated or has generic or common cause implications (as defined in NUREG/CR-4780, Ref. 9).

Finally, the monitoring program should identify any corrective actions to preclude recurrence of unacceptable failures or degraded performance below expectations. The circumstances surrounding the failure may indicate that the SSC failed because of adverse or harsh operating conditions (e.g., operating a valve dry, over-pressurization of a system) or failure of another component which caused the SSC failure. Therefore, corrective actions should also consider SSCs with similar characteristics with regard to operational, design, or maintenance conditions.

It is expected that upon initial approval of the proposed monitoring program, subsequent NRC oversight will focus on evaluating performance results rather than on a programmatic review.

2.6 Element 4: Submit Proposed Change

Requests for proposed change to the plant's CLB typically take the form of requests for license amendments (including changes to or removal of license conditions), technical changes, changes to or withdrawals of orders, and changes to programs pursuant to 10 CFR 50.54 (e.g., QA program changes under 10 CFR 50.54(a)). Licensees should: (i) carefully review the proposed CLB change in order to determine the appropriate form of the change request, and (ii) assure that information required by the relevant regulations(s) in support of the request is developed; and (iii) prepare and submit the request in accordance with relevant procedural requirements. For example, license amendments should meet the requirements of 10 CFR §§50.90, 50.91 and 50.92, as well as the procedural requirements in 10 CFR §50.4. Where the licensee submits risk information in support of the CLB change request, that information should meet the guidance in Section 3 of this regulatory guide.

Licensees are free to decide whether to submit risk information in support of their CLB change request. Where the licensee's proposed change to the CLB is consistent with currently-approved staff positions, the staff's determination will be based solely on traditional deterministic engineering analysis without recourse to risk information (although the staff may consider any risk information which is submitted by the licensee). However, where the licensee's proposed change goes beyond currently-approved staff positions, the staff will normally consider both information based upon traditional deterministic engineering analysis as well as information based upon risk insights. If the licensee does not submit risk information in support of a CLB change which goes beyond currently-approved staff positions, the staff may request the licensee to submit such information. Such an information request is not a backfit under 10 CFR 50.109. If the licensee chooses not to provide the risk information, the staff will review the proposed application using deterministic engineering analysis and determine whether sufficient information has been provided to support the requested change.

In developing the risk information set forth in this regulatory guide, licensees will likely identify SSCs with high risk significance which are not currently subject to regulatory requirements, or are subject to a level of regulation which is not commensurate with their risk significance. It is expected that licensees will propose CLB changes that will subject these SSCs to appropriate level of regulation, consistent with the risk significance of each SSC. Specific information on the staff's expectations are set forth in the application-specific regulatory guides.

2.7 Quality Assurance

As stated in Section 2.4, the staff expects that the quality of the engineering analyses conducted to justify proposed CLB changes will be appropriate for the nature of the change. In this regard, it is expected that for traditional engineering analyses (e.g., deterministic engineering calculations) existing provisions for quality assurance (e.g., 10CFR50, Appendix B for safety-related SSCs) will apply and provide the appropriate quality needed. Likewise, when a risk assessment of the plant is used to provide insights into the decisionmaking process, the staff expects that the PRA will have been subject to quality control.

To the extent that a licensee elects to use PRA information to enhance or modify activities affecting the safety-related functions of SSCs, the following, in conjunction with the other guidance contained in this guide, describe an acceptable way to ensure that the pertinent quality assurance requirements of 10CFR50, Appendix B are met and that the PRA is of sufficient quality to be used for regulatory decisions:

- utilize personnel qualified for the analysis
- utilize procedures that ensure control of documentation, including revisions, and provide for independent review, verification or checking of calculations and information used in the analyses (an independent peer review can be used as an important element in this process)
- provide documentation and maintain records in accordance with the guidelines in Section 3 of this guide
- provide for an independent audit function to verify quality (an independent peer review can be used for this purpose)
- utilize procedures that ensure appropriate attention and corrective actions are taken if analyses or information used in previous decision making is determined to be in error.

Where performance monitoring programs are used in the implementation of proposed change to the CLB, it is expected that those programs will be implemented utilizing quality provisions commensurate with the safety significance of affected SSCs. An existing PRA or analyses can be utilized to support a proposed CLB change, provided it can be shown that the appropriate quality provisions have been met.

3. DOCUMENTATION AND SUBMITTAL

3.1 Introduction

To permit the staff's audit to ensure that the analyses conducted were sufficient to conclude that the key principles of risk-informed regulation have been met, documentation of the evaluation process and findings are expected to be maintained. Additionally, information submitted should include a description of the process used by the licensee to ensure quality and some specific information to support the staff's conclusion regarding the acceptability of the requested CLB change.

3.2 Documentation

Archival documentation should include a detailed description of engineering analyses conducted and the results obtained, irrespective of whether they were quantitative or qualitative, or whether the analyses made use of traditional engineering methods or probabilistic approaches. This documentation should be maintained by the licensee, as part of their normal quality assurance program, so that it is available for examination. Documentation of the analyses conducted to support changes to a plant's CLB should be maintained as lifetime quality records in accordance with Regulatory Guides 1.33 and 1.88 (Ref. 10 and 11, respectively). An example of typical PRA documentation is described in draft NUREG-1602.

3.3 Licensee Submittal

To support the staff's conclusion that the proposed CLB change is consistent with the key principles of risk-informed regulation and NRC staff expectations, the following information is expected to be submitted to the NRC:

- a description of how the proposed change will impact the CLB (Relevant principle: CLB changes meet regulations.)
- a description of the components and systems affected by the change, the type of changes proposed, the reason for the changes, and results and insights from an analysis of available data on equipment performance (Relevant staff expectation: All safety impacts of the proposed CLB change shall be evaluated.)
- a tabulation of the current licensing basis accident parameters that are affected by the change and an assessment of the expected changes (Relevant principles: CLB changes meet the regulations; sufficient safety margins are maintained; defense-in-depth is maintained.)
- a reevaluation of the licensing basis accident analysis and the provisions of 10 CFR Parts 20 and 100, if appropriate (Relevant principles: CLB changes meet the regulations; sufficient safety margins are maintained; defense-in-depth is maintained.)

Draft for Comment

Documentation

- an evaluation of the impact of the change in licensing bases on the breadth or depth of defense-in-depth attributes of the plant (Relevant principle: Defense-in-depth is maintained.)
- identification of how and where the proposed change will be documented as part of the plants licensing basis (e.g., FSAR, TS, licensing conditions). This should include proposed changes and/or enhancements to the regulatory controls for high risk-significant SSCs which are not subject to any requirements, or where the requirements are not commensurate with the SSCs risk-significance.
- The licensee should also identify:
 - those key assumptions in the PRA, elements of the monitoring program, and commitments made to support the application
 - those SSC's for which requirements should be increased
 - a description of that information to be provided as part of the plants licensing basis (e.g., FSAR, TS, licensing condition)

The licensee's submittal should discuss measures used to ensure adequate quality, such as a report that addresses the appropriateness of the PRA model for supporting a risk assessment of the CLB change under consideration. An independent peer review can be an important element of ensuring this quality. The report should address any analysis limitations that are expected to impact the conclusion regarding acceptability of the proposed change. The licensee's resolution of the findings of the peer review, when performed, should also be submitted. For example, this response could indicate whether the PRA was modified or a justification as to why no change was necessary to support decisionmaking for the CLB change under consideration. As discussed in Section 2.4.2, the staff's decision on the proposed license amendment will be based on its independent judgment and review, as appropriate, of the entire application.

In order to have confidence that the risk assessment conducted is adequate to support the conclusion that there is no more than an insignificant increase in risk to health and safety of the public has been met, a **summary of the risk assessment methods** used should be submitted. Consistent with current practice, information submitted to the NRC for its consideration in making risk-informed, regulatory decisions will be made publicly available, unless such information is deemed proprietary and justified as such. The following information should be submitted and is intended to illustrate that the scope and quality of the engineering analyses conducted to justify the proposed CLB change is appropriate to the nature and scope of the change:

- a description of risk assessment methods used
- the key modeling assumptions
- the success criteria and the basis for each
- a list of initiators considered and their frequencies, as well as the basis for excluding any initiators from the risk assessment

- a listing of systems and components addressed in the risk assessment, the failures considered for each and the basis for excluding failures, and the dependencies between systems and components
- the event trees and fault trees as necessary to support the analysis
- a lists of operator actions modeled in the PRA (and the basis for excluding operator actions) and their error probabilities
- a list describing all events included in the risk assessment

Submitted information summarizing the results of the risk assessment should include:

- a description of dominant sequences
- an estimate of total plant CDF (including a qualitative or quantitative assessment of uncertainty) before and after implementing the proposed CLB change
- an estimate of containment performance as described by plant damage states and the frequencies of the high and low consequence categories (if a simplified Level 2 PRA analysis was performed such as is described in Appendix B to this regulatory guide); or frequencies of accident progression pathways (including a qualitative or quantitative assessment of uncertainty), as grouped for source term calculations, if a full Level 2 PRA was conducted
- the definition of source terms and an identification of their frequencies and magnitudes (including uncertainty) if full Level 2/3 PRA was performed
- the frequencies of individual early and latent fatalities, if a full Level 2/3 analysis was performed

In addition, information that should be submitted as part of the justification for the specific CLB change includes:

- a description of the analyses performed to assess the impact of the change on risk
- an estimate of plant CDF and LERF and changes in those estimates if the proposed CLB change were implemented
- an identification of all minimal cutsets affected by the change, any success criteria that are affected by the change, and any changes in dominant risk contributors

Documentation

- the results of analyses that show that the conclusions regarding the impact of the CLB change on plant risk will not vary significantly under a different set of assumptions. (See NUREG-1602 for a discussion of the uses and limitations of importance measures and sensitivity studies.)

The staff also expects licensees to track and consider the cumulative impact of all plant changes, including those not submitted for NRC review and approval.

3.4 Implementation Plan and Performance Monitoring Process

As described in Section 2.5 above, a key principle of risk-informed regulation is that proposed performance implementation and monitoring strategies reflect uncertainties in analysis models and data. Consequently, the submittal should include a description and rationale for the implementation and performance monitoring strategy for the proposed CLB change.

4. REFERENCES

1. Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement, U.S. Nuclear Regulatory Commission, 60FR42622
2. Use of PRA in Risk-Informed Applications, U.S. Nuclear Regulatory Commission, Draft NUREG-1602, February 1997
3. An Approach for Plant-Specific, Risk-Informed Decisionmaking: Inservice Testing, U.S. Nuclear Regulatory Commission, Draft Regulatory Guide DG-1062, February 1997
4. An Approach for Plant-Specific, Risk-Informed Decisionmaking: Inservice Inspection, U.S. Nuclear Regulatory Commission, Draft Regulatory Guide DG-1063, March 1997
5. An Approach for Plant-specific, Risk-Informed Decisionmaking: Graded Quality Assurance, U.S. Nuclear Regulatory Commission, Draft Regulatory Guide DG-1064, February 1997
6. An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications, U.S. Nuclear Regulatory Commission, Draft Regulatory Guide DG-1065, February 1997
7. Industry Guidelines for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants, NUMARC 93-01 Rev. 1, January 1996
8. Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG-1150, December 1990
9. Procedures for Treating Common Cause Failures in Safety and Reliability Studies, NUREG/CR-4780, January 1989
10. Quality Assurance Program Requirements, U.S. Nuclear Regulatory Commission, Regulatory Guide 1.33, February 1978
11. Collection, Storage, and Maintenance of Nuclear Power Plant Quality Assurance Records, U.S. Nuclear Regulatory COMMISSION, Regulatory Guide 1.88
12. PSA Applications Guide, D. True et al., EPRI TR-105396, August 1995

APPENDIX A: USE OF RISK IMPORTANCE MEASURES TO CATEGORIZE STRUCTURES, SYSTEMS, AND COMPONENTS WITH RESPECT TO SAFETY SIGNIFICANCE

Introduction

For several of the proposed applications of the risk-informed regulation process, one of the principal activities is the categorization of SSCs and human actions according to safety significance. The purpose of this Appendix is to discuss one way that this categorization may be performed to be consistent with principle 4 and the expectations discussed in Section 2.1.

Safety-significance of an SSC can be thought of as being related to the role the SSC plays in preventing the occurrence of the undesired end state. Thus the position adopted in this regulatory guide is that all the SSCs and human actions considered when constructing the PRA model (including those that do not necessarily appear in the final quantified model, either because they have been screened initially, assumed to be inherently reliable or have been truncated from the solution of the model) have the potential to be safety significant, since they play a role in preventing core damage.

In establishing the categorization, it is important to recognize the purpose behind the categorization, which is, generally, to sort the SSCs and human actions into groups according to those for which some relaxation of requirements is proposed, and those for which no such change is proposed. It is the proposed application that is the motivation for the categorization, and it is the potential impact of the application on the particular SSCs and human actions and on the measures of risk which ultimately determines which of the SSCs and human actions must be regarded as safety-significant within the context of the application. This impact on overall risk must be evaluated in light of the principles and decision criteria identified in this draft guide. Thus, the most appropriate way to address the categorization is through a requantification of the risk measures.

However, the feasibility of performing such risk quantification has been questioned for those applications for which a method for the evaluation of the impact of the change on SSC unavailability is not available. An acceptable alternative to requantification of risk is for the licensee to perform the categorization of the SSCs and human actions in an integrated manner, making use of an analytical technique, based on the use of PRA importance measures, as input. This appendix discusses the technical issues associated with the use of PRA importance measures. NUREG-1602 includes more detailed discussion of this subject.

Technical Issues Associated with the Use of Importance Measures

In the implementation of the Maintenance Rule and in industry guides for the risk-informed applications (for example, the PSA Applications Guide), the Fussell-Vesely Importance, Risk Reduction Worth, and Risk Achievement Worth are the most commonly identified measures in the relative risk ranking of SSCs.

Draft for Comment

Appendix A

However, in the use of these importance measures for risk-informed applications, there are several issues that should be addressed. Most of the issues are related to technical problems which can be resolved by the use of sensitivity studies or by appropriate quantification techniques. These issues are discussed in detail in the subsection below. In addition, there are two issues, namely a) that risk rankings apply only to individual contributions and not to combinations or sets of contributors, and b) that risk rankings are not necessarily related to the risk changes which result from those contributor changes, that the licensee should be aware of and should make sure that they have been addressed adequately. When performed and interpreted correctly, component-level importance measures can provide valuable input to the licensee.

Risk ranking results from a PRA can be affected by many factors, the most important being model assumptions and techniques (e.g., for modeling of human reliability or common cause failures), the data used, or the success criteria chosen. The licensee should therefore make sure that the PRA is of sufficient quality.

In addition to the use of a "quality" PRA, the robustness of categorization results should also be demonstrated for conditions and parameters that might not be addressed in the base PRA. Therefore, when importance measures are used to group components or human actions as low safety-significant contributors, the information to be provided to the analysts performing qualitative categorization should include sensitivity studies and/or other evaluations to demonstrate the sensitivity of the importance results to the important PRA modeling techniques, assumptions, and data. Issues that should be considered and addressed are listed below.

Truncation limit: The licensee should determine that the truncation limit has been set 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. Depending on the PRA level of detail (module level, component level, or piece-part level), this may translate into a truncation limit from $1\text{E-}12$ to $1\text{E-}8$ per reactor year. In addition, the truncated set of minimal cutsets should be determined to contain the important application-specific contributors and their logical combinations.

Risk metrics: The licensee should ensure that risk in terms of both CDF and LERF is considered in the ranking process.

Completeness of risk model: The licensee should ensure that the PRA model is sufficiently complete to address all important modes of operation for the SSCs being analyzed. Safety significant contributions from internal events, external events, and shutdown and low power initiators should be considered either by using PRA or other engineering analyses. (NUREG-1602 provides a discussion of model completeness.)

Sensitivity analysis for component data uncertainties: The sensitivity of component categorizations to uncertainties in the parameter values should be addressed by the licensee. Licensees should be satisfied that SSC categorization is not affected by data uncertainties.

Sensitivity analysis for common cause failures: CCFs are modeled in PRAs to account for dependent failures of redundant components within a system. The licensee should determine that the safety significant categorization has been performed taking into account the combined effect of associated basic PRA events, such as failure to start and failure to run, including indirect contributions through associated CCF event probabilities. CCF probabilities can affect PRA results by enhancing or obscuring the importance of

components. 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.

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 affected 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. The licensee should ensure that the categorization has not been unduly affected by the modeling of recovery actions.

Multiple component considerations: As discussed previously, importance measures are typically evaluated on an individual SSC or human action basis. One potential concern raised by this is that single-event importance measures have the potential of dismissing all elements of a system or group despite the system or group having a high importance when taken as a whole. (Conversely, there may be grounds for screening out groups of SSCs, owing to the unimportance of the systems of which they are elements.) There are two potential approaches to addressing the multiple component issue. The first is to define suitable measures of system or group importance. The second is to choose appropriate criteria for categorization based on component-level importance measures. In both cases, it will be necessary for the licensee to demonstrate that the cumulative impact of the change has been adequately addressed.

While there are no widely-accepted definitions of system or group importance measures, if any are proposed, the licensee should make sure that the measures are capturing the impact of changes to the group in a logical way. As an example of the issues that arise consider the following. For front-line systems, one possibility would be to define a Fussell-Vesely type measure of system importance as the sum of the frequencies of sequences involving failure of that system, divided by the sum of all sequence frequencies. Such a measure would need to be interpreted carefully if the numerator included contributions from failures of that system due to support systems. Similarly, a Birnbaum-like measure could be defined by quantifying 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. However, again the support systems make the situation 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.

In the absence of appropriately defined group level importance measures, reliance must be made on a qualitative categorization by the licensee, as part of the integrated decisionmaking process, to make the appropriate determination.

Relationship of Importance Measures to risk changes: Importance measures do not directly relate to changes in risk. Instead, the risk impact is indirectly reflected in the choice of the value of the measure used to determine whether an SSC should be classified as being of high and low safety significance. This is a

Draft for Comment

Appendix A

concern whether importances are evaluated at the component or at the group level. The PSA Applications Guide suggested values of Fussell-Vesely importance of .05 at the system level, and .005 at the component level for example. However, the criteria for categorization into low and high significance should be related to the acceptance criteria for changes in CDF and LERF. This implies that the criteria should be a function of the base case CDF and LERF rather than being fixed for all plants. Thus the licensee should demonstrate how the choice of criteria are related to, and conform with, the acceptance guidelines described in this document. If component level criteria are used, they should be established taking into account that the allowable risk increase associated with the change should be based on simultaneous changes to all members of the category.

SSCs not included in the final quantified cutset solution: Importance measures based on the quantified cutsets will not factor in those SSCs that have either been truncated, or were not included in the fault tree models because they were screened on the basis of high reliability. SSCs that have been screened because their credible failure modes would not fail the system function can be argued to be unimportant. The licensee must make sure that these SSCs are considered. This subject is discussed in more detail in NUREG-1602.

APPENDIX B: AN APPROACH FOR ESTIMATING THE FREQUENCIES OF VARIOUS CONTAINMENT FAILURE MODES AND BYPASS EVENTS

B.1 Introduction

This appendix describes an approach for estimating the frequencies of various containment failure modes and bypass events. This approach is designed to supplement Level 1 PRAs submitted in support of risk-informed decisionmaking. The intent is to use accident sequence information provided in the Level 1 PRA to estimate the frequencies of various plant damage states (PDSs) and hence the frequencies of containment failure and bypass.

Accident sequences leading to core damage are usually grouped into PDS for the purpose of assessing the subsequent accident progression. A PDS is defined in such a way that all accident sequences binned into it can be treated identically on the accident progression analysis. That is, the PDS definition must recognize all distinctions that matter in the accident progression analysis. Once a set of PDSs is defined for a given reactor, containment performance is calculated for each PDS. It is clear that some PDSs will be more challenging to containment integrity than others (pressure, temperature, mechanical loading, etc.), and some PDSs will completely bypass containment. For example, an interfacing systems LOCA has the potential to completely bypass containment, while a transient event with loss of containment heat removal (CHR) will pose more of a challenge to containment integrity than a LOCA with the CHR systems operating. The PDSs are distributed into various containment failure modes (CFMs) to allow for assessment of the likely outcomes of the accident progression.

For the purpose of the simplified approach, sufficient Level 2 PRAs have been completed to permit the allocation of core damage accident sequences to appropriate CFMs. To allow comparison to the acceptance guidelines identified in this appendix, the approach has to distinguish between containment failure modes that might lead to early fatalities vs. those failure modes that will not cause early fatalities. Consequently, the failure modes were categorized as follows:

- early containment failure or bypass (potentially leading to large early release, i.e., early fatalities likely)
- late containment failure or containment intact (potentially not leading to large early release, i.e., early fatalities unlikely)

Once established, the frequencies of these categories can be determined and changes in the frequencies compared against the acceptance guidelines. A key advantage of this approach is that each accident sequence is allocated to a risk category based on the status of the plant. A scheme for allocating the various accident sequences to the categories is described below. An event tree has been developed for each containment type that allocates accident sequences to one of the categories. The intent is that each licensee will develop split fractions for most of the questions in the trees based on plant-specific accident sequences and characteristics. These trees prescribe a single question concerning the likelihood of early containment failure.

Each accident sequence from the Level 1 analysis can be processed through the trees with individual frequencies allocated to the various release categories. The sum of these individual accident frequencies determines the total frequency for each release category.

B.2 PWRs With Large Volume Containments

Figure B-1 presents an event tree that allows allocation of accident sequences to one of two categories for use with PRAs for PWRs with large dry or subatmospheric containments. Each accident sequence in a Level 1 PRA would be allocated to one of these categories based on the plant status as defined by the various accident sequences. This

approach prescribes only a single question concerning the likelihood of containment failure at vessel breach (i.e., Question 5). The split fraction for this question reflects a reasonable estimate of the likelihood of early containment failure for large-volume containments given a high-or-low pressure core meltdown accident. However, if a licensee has justification for an alternative split fraction, this could be provided to support changes in the event tree quantification.

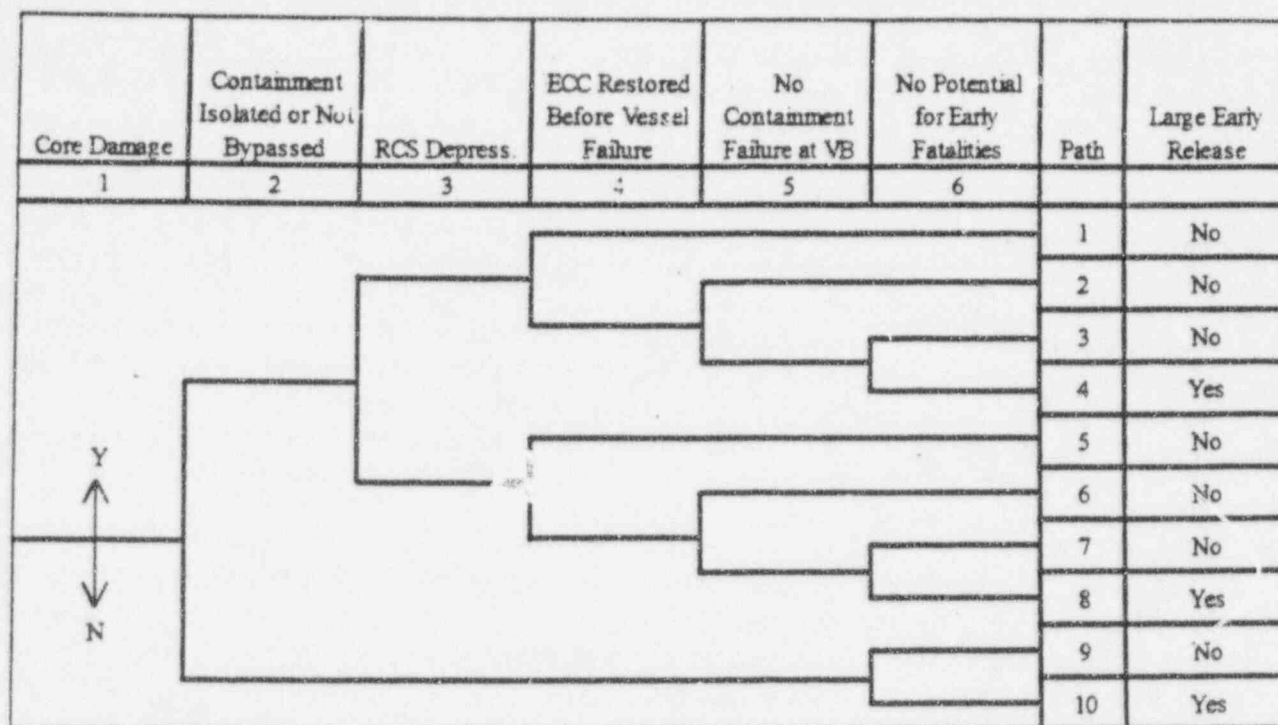


Figure B-1 PWR Large Dry Containments

*Note: In the case of seismic initiators, there is a possibility that effective warning and evacuation may be precluded due to the disruption of warning systems and evacuation paths. If the containment structure is predicted to survive the event, the likelihood of long-term containment heat removal should be investigated. If CHR is predicted to fail (for any set of reasons) the containment will eventually fail due to over pressurization and, the consequence category should be "yes" since it is unlikely that evacuation will occur.

Question 1: Core Damage Frequency?

This is simply the entry point for the tree. The frequency for the accident sequence under consideration is entered here.

Question 2: Containment Isolated or Not Bypassed?

This question includes accidents in which the containment fails to isolate, as well as accidents initiated by containment bypass (such as interfacing systems LOCAs and steam generator tube ruptures). This category is intended to apply only to accidents that bypass containment at accident initiation. Accident sequences that cause containment bypass (such as induced SGTR) during accident progression after core damage are not

included in this category. Accidents in which the containment is initially open have been found important during shutdown and would also be included in this category.

Question 3: RCS Depressurized?

For accidents initiated by transients and small break LOCAs, the RCS will remain at high pressure unless the operators depressurize the RCS or the RCS pressure boundary fails. If the operators cannot depressurize the RCS the accident sequence would be allocated to the "not depressurized branch" in the event tree. However, a licensee may wish to take credit for hot leg failure as a cause of RCS depressurization before vessel breach. Justification should be provided if such a failure mechanism is assumed. Intermediate and large -break LOCAs and accidents in which the operators depressurize the primary system to below 200 psi would be allocated to the depressurized branch.

Question 4: ECC Restored Before Vessel Breach?

Accidents in which ECC is restored within 30 minutes of the start of core damage are assumed to arrest the accident progression without vessel breach. For these accidents, subsequent questions related to containment failure at vessel breach and the potential for early fatalities are not pertinent. If the ECC is not restored within 30 minutes, vessel breach is assumed to occur, and all subsequent questions are pertinent.

Credit for in-vessel arresting of the accident will only be given for cases where recovering AC power will lead to the restoration of ECCS within 30 minutes of the onset of core damage. For example, no credit will be given for an operator manually depressurizing the reactor and using a low-pressure system between core damage and vessel breach. If cooling is restored within 30 minutes, the probability of successful arrest is assumed to be 1.0; if cooling is restored after 30 minutes, the probability of successful arrest is assumed to be 0.0.

Question 5: No Containment Failure at Vessel Breach?

The likelihood of containment failure at vessel breach depends on several factors, such as the pressure in the primary system, the amount and temperature of the core debris exiting the vessel, the size of the hole in the vessel, the amount of water in the cavity, the configuration of the cavity, and the structural capability of the containment building. In the simplified event tree, only the pressure in the primary system is distinguished so that all other considerations have to be folded into the split fractions for high- and low-pressure sequences. Each possibility is discussed below.

Low-pressure Sequences?

Under these circumstances, various mechanisms could challenge containment integrity. These include in-vessel steam explosions, rapid steam generation caused by core debris contacting water in the cavity, and hydrogen combustion. On the basis of previous PRAs, the probability of early containment failure is assumed to be 0.01. If a licensee does not consider this probability to be appropriate because of plant-specific considerations, then the probability can be changed, but justification for the change should be provided.

High-Pressure Sequences?

Several mechanisms could challenge containment under these circumstances. In-vessel steam explosions are a potential failure mechanism, but it is more difficult to trigger steam explosions at high pressure than at low pressure. Steam generator tube rupture is also possible because of high temperatures and pressures during core meltdown. If induced SGTR occurs, a potential bypass of containment can result if the secondary system is

Appendix B

open. However, the most important failure mechanisms for high-pressure core meltdown sequences are associated with high pressure melt ejection (HPME). Ejection of the core debris at high-pressure can cause the core debris to form fine particles that can directly heat the containment atmosphere (i.e., DCH) and cause rapid pressure spikes. During HPME, the hot particles could also ignite any combustible gases in containment, thereby adding to the pressure pulse. The potential for DCH to cause containment failure depends on several factors, such as the primary system pressure, the size of the opening in the vessel, the temperature and composition of the core debris exiting the vessel, the amount of water in the cavity, and the dispersive characteristics of the reactor cavity. The probability of early containment failure is, therefore, a composite of each of these potential failure modes and is assumed to be 0.1. Again, a licensee can change this probability, provided that appropriate justification is provided.

The fraction of low- or high-pressure sequences that result in early containment failure at the time of the vessel breach have the potential to be allocated to the high-release category. The remaining fractions of the accident sequences (in which the containment remains intact) are allocated to the low-release category.

Question 6: No Potential for Early Fatalities?

The potential for early fatalities depends on the magnitude and timing of the release relative to two factors:

- (1) the time elapsed from reactor scram to the time at which the release starts (particularly relevant to shutdown accidents).
- (2) the time from the declaration of a general emergency to the time of the start of the release compared to the time required to effectively warn and evacuate the population in the vicinity of the plant.

During shutdown, for example, the early health risk from many internally initiated accidents is greatly reduced simply by the decay of the short-lived isotopes that affect early fatalities. At full-power operation, this question allows long-term sequences, such as loss of CHR or other late over pressurization sequences to be placed in the low-release category without the need for a detailed evaluation of the ultimate containment response, since it is assumed that evacuation will occur before the release starts. Sequences originating from seismic initiators should all be associated with the potential for early fatality branch on the event tree. In order to place a sequence on the branch labeled no potential for early fatalities, a licensee should provide information, specific to the sequence, concerning when a general emergency would be declared and the expected time required to warn and evacuate the population.

For shutdown accidents, where the containment is essentially unisolated, the time available for evacuation is the time from declaration of a general emergency to the onset of core damage. For accidents at full power, the time available for evacuation is the time from the declaration of a general emergency to vessel breach. Unless otherwise justified, the licensee should use one hour from onset of core damage to vessel breach.

All Other Accidents

All accident sequences that do not fall into the above categories are assumed not to fail containment and, therefore, are allocated to the no "large early release" consequence bin category.

B.3 PWR Ice Condenser Containments

Figure B-2 provides a high-level containment event tree (CET) for ice condenser plants. As with large dry containments, outcomes of the CET for ice condenser plants are placed in a high consequence category if early failure occurs and the potential exists for early fatalities. Late failures, which generally occur as a result of failure of the long-term CHR systems, and on all other accidents are assigned a low consequence category. (There is considerable similarity in the event trees for large dry and ice condenser containments, and many of the questions are similar.)

Question 1: Core Damage Frequency?

This is simply the entry point for the event tree. The frequency of the accident sequence under consideration is entered here.

Question 2: Containment Isolated or Not Bypassed?

This top event is similar to the first question asked in the event tree for large dry containments; a negative answer results in an outcome with the potential to be allocated to the "large early release" consequence category.

Question 3: Hydrogen Igniters Operating Before Core Damage?

The smaller volume containments, such as ice condensers, are critically dependent on the availability of hydrogen igniters to control pressure loads resulting from hydrogen combustion involving both static and dynamic loads. The annular design of the ice compartments lends itself to build up of hydrogen concentrations. There is a significant probability of a hydrogen combustion event causing containment failure if the igniters are not operating (regardless of whether core cooling was restored).

Question 4: RCS Depressurized?

If the RCS cannot be depressurized by operator action, core melt with the RCS remaining at high pressure will pose a severe threat to the containment integrity. For ice condenser plants, this can lead to HPME and DCH or impingement of the core debris on the containment wall in the seal table room, provided this vulnerability exists at the plant.

Question 5: ECC Restored Before Vessel Failure?

All accidents in which ECC is restored within 30 minutes of the start of core damage are assumed to arrest the accident progression without vessel breach. For these accidents, if the igniters are not operating there is the possibility of containment failure due to hydrogen combustion even if the core is retained in the vessel. If the igniters are operating, then it is assumed that the containment does not fail due to hydrogen combustion. If the ECC is not restored within 30 minutes, then vessel breach is assumed to occur. Credit for in-vessel arrest of the accident will only be given for cases where recovering AC power will lead to the restoration of ECCS within 30 minutes of the onset of core damage. For example, no credit will be given for an operator manually depressurizing the reactor and using a low pressure system to inject water between core damage and vessel breach. If cooling is restored within 30 minutes, the probability of successful arrest is assumed to be 1.0, and if cooling is restored after 30 minutes, the probability of successful arrest is assumed to be 0.0.

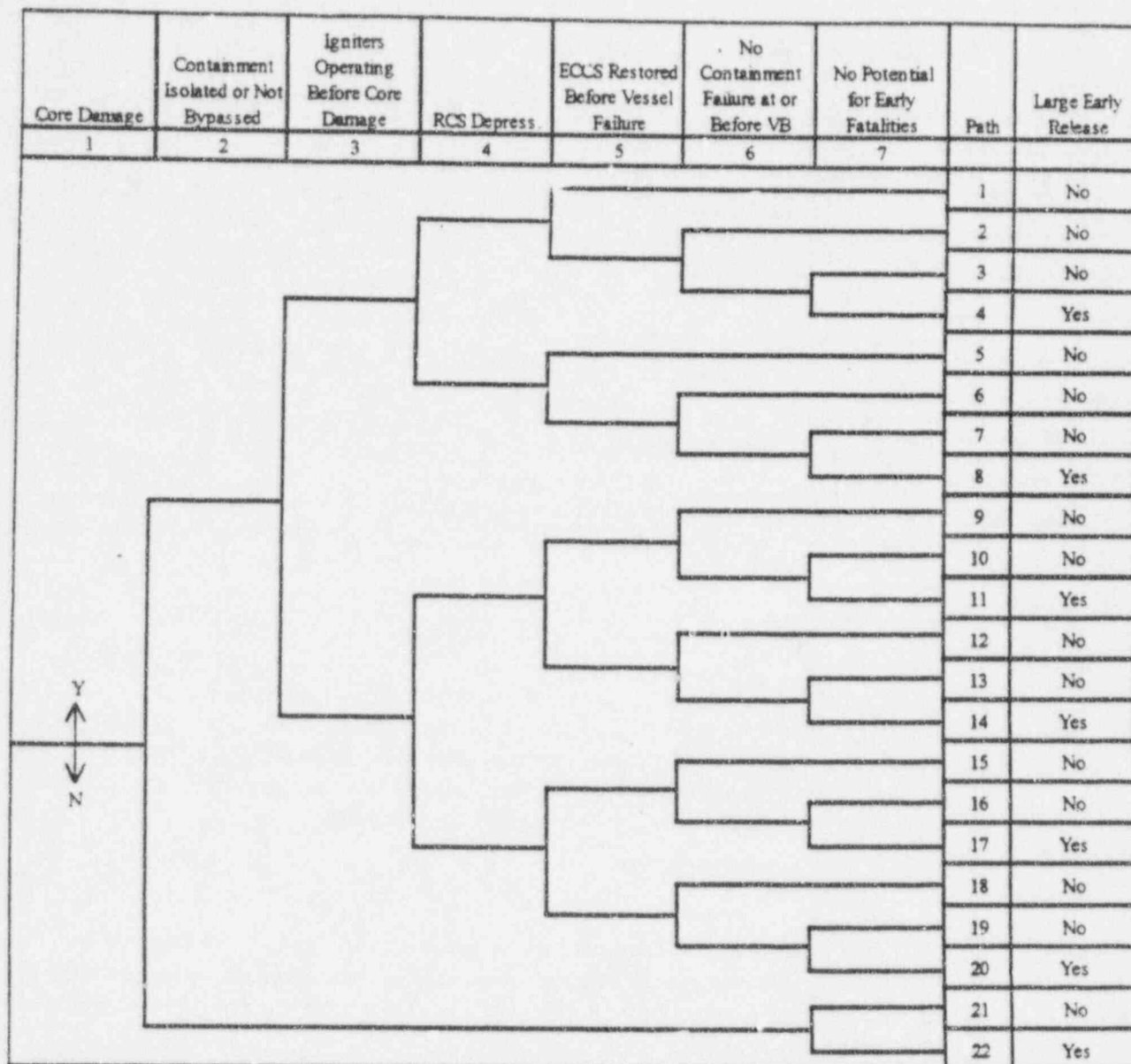


Figure B-2 PWR Ice Condenser Containments

*Note: In the case of seismic initiators, there is a possibility that effective warning and evacuation may be precluded due to the disruption of warning systems and evacuation paths. If the containment structure is predicted to survive the event, the likelihood of long-term containment heat removal should be investigated. If CHR is predicted to fail (for any set of reasons) the containment will eventually fail due to over pressurization and, the consequence category should be "yes" since it is unlikely that evacuation will occur.

Question 6: No Containment Failure at or Before Vessel Breach?

If the igniters are not operating, then the potential exists for failure of the containment as a result of hydrogen combustion before the vessel breach. This failure can, therefore, occur even if the core damage is arrested in the vessel. The probability of a hydrogen combustion event causing containment failure before the vessel

breach was determined to be 0.04. Again, if a licensee wishes to change this probability, appropriate justification should be provided. If the igniters are operating, the containment is assumed not to fail before the vessel.

As for the Large Dry containments, the likelihood of containment failure at vessel breach depends on several factors, such as the pressure in the primary system, the amount and temperature of the core debris exiting the vessel, the size of the hole in the vessel, whether or not the igniters are operating, the amount of ice left in the ice chests, the amount of water in the cavity, the configuration of the cavity, and the structural capability of the containment building. In the simplified event tree in Figure B-2, the pressure in the primary system, and the operability of the igniters, are considered so that all other considerations have to be folded into the appropriate split fractions in the event tree. Each possibility is discussed below.

Low Pressure Sequences?

Under these circumstances, various of mechanisms could challenge containment integrity including in-vessel steam explosions, rapid steam generation caused by core debris contacting water in the cavity, and hydrogen combustion. For ice condenser containments, the likelihood of these failure modes depends upon the operability of the igniters and the availability of ice in the condenser. On the basis of previous PRAs, the probabilities of early containment failure at or before vessel breach, with and without the igniters operating are given below:

| | Igniters Operating | Igniters Failed |
|--|--------------------|-----------------|
| Probability of Early Containment Failure | 0.01 | 0.1 |

If a licensee considers either of these probabilities to be inappropriate because of plant-specific considerations, the probabilities can be changed, but justification for the changes should be provided.

High-Pressure Sequences?

Ice condenser containments can be challenged by failure modes similar to those considered for large volume containments. In-vessel steam explosions are a potential failure mechanism, but it is more difficult to trigger steam explosions at high pressure than at low pressure. Steam generator tube rupture is also possible because of high temperatures and pressures during core meltdown. If induced SGTR occurs, a potential bypass of containment can result if the secondary system is open. However, two important failure mechanisms are associated with HPME in ice condenser containments. The potential for DCH to cause failure of ice condenser containments depends on those factors found important for large volume containments. However, ice remaining in the ice chest was also found to mitigate DCH for ice condenser containments. The second failure mechanism associated with HPME in ice condenser containments is impingement of corium on the containment wall, which can lead to failure and a direct path out of containment. Another important failure mechanism for ice condenser containments is hydrogen combustion at the time of vessel failure. The importance of this failure mechanism depends on the operability of the igniters.

The probability of early containment failure at or before vessel breach is, therefore, a composite of each of these potential failure modes as indicated below:

| | Igniters Operating | Igniters Failed |
|--|--------------------|-----------------|
| Conditional Probability of Early Containment Failure | 0.05 | 0.2 |

Again, a licensee can change the above probabilities, provided that appropriate justification is furnished.

The fraction of low- or high-pressure sequences that result in early containment failure at the time of vessel breach have the potential to be allocated to the large early release category. The remaining fractions of the accident sequences (in which the containment remains intact) are allocated to the no "large early release" consequence category.

Question 7: No Potential for Early Fatalities?

The potential for early fatalities depends on the magnitude of the release and on the timing of the release relative to two factors: (1) the time elapsed from reactor scram to the time at which the release starts (particularly relevant to shutdown accidents) and (2) the time from the declaration of a general emergency to the time of the start of the release compared to the time required to effectively warn and evacuate the population in the vicinity of the plant. During shutdown, for example, the early health risk from many internally initiated accidents is greatly reduced due simply to the decay of the short-lived isotopes which affect early fatalities. At full power operation, this question allows long-term sequences, such as loss of CHR or other late over pressurization sequences to be placed in the low release category without the need for a detailed evaluation of the ultimate containment response, since it is assumed that evacuation will occur before the release starts. Sequences originating from seismic initiators should all be placed on the potential for early fatality branch on the event tree. In order to place a sequence on the branch labeled "no potential for early fatalities," a licensee should provide information, specific to the sequence, concerning when a general emergency would be declared and the expected time required to warn and evacuate the population. For shutdown accidents, where the containment is essentially unisolated, the time available for evacuation is the time from declaration of a general emergency to the onset of core damage. For accidents at full power, the time available for evacuation is the time from the declaration of a general emergency to vessel breach. Unless otherwise justified, the licensee should use one hour from onset of core damage to vessel breach.

B.4 BWR Mark I Containment

Figure B-3 provides an event tree allowing allocation of accident sequences to one of two consequence categories for use with PRAs for BWRs with Mark I containments. The structure of the event tree is based on the premise that all early releases that are scrubbed by the suppression pool are sufficiently low that by themselves will not result in individual early fatality risk. Hence, if an early failure occurs with the functionality of the suppression pool intact, it is assumed that the early scrubbed releases will not pose an early fatality threat to the population within one mile of the plant boundary, and that this population will evacuate before substantial core concrete interaction releases or late iodine releases from pools are of a magnitude to cause individual early fatality risk (except in the case of a seismic event, as noted in Figure B-5). Each top event question in the event tree is discussed below. The licensee would be expected to provide the split fractions for all questions with the exception of Question 7.

Question 1: Core Damage Frequency?

This is simply the entry point for the event tree. The frequency for the accident sequence under consideration is entered here.

Question 2: Containment Failed/Vented Prior to VB (Releases not scrubbed by suppression pool)?

This question involves the fraction of the core damage frequency where the containment is failed at the start of the accident or prior to vessel failure. Failures at the start of the accident include bypass sequences (Event V), containment isolation failures, and sequences where the containment is initially open. For example, during cold shutdown and refueling, if the containment is open and the vessel head is removed, no credit should be given for closing the containment in the presence of the radioactive environment within the containment. Failures after the start of the accident can also occur due to insufficient containment heat removal, e.g., during ATWS or loss of containment heat removal. Loss of containment heat removal or other non-ATWS sequences where the only breach of containment integrity prior to vessel failure is through wetwell vents should be put into the "OK" category.

Question 3: Core Damage Arrested Prior to Vessel Failure?

This question accounts for the fact that some sequences may be arrested in-vessel without significant releases from the RPV. All arrested sequences are assigned to the Low consequence category. Shutdown events where the vessel head has been removed should all be placed in the "Breach" category. Credit for in-vessel arresting of the accident will only be given for cases where recovering AC power will lead to the restoration of ECCS within 30 minutes of the onset of core damage. For example, no credit will be given for an operator manually depressurizing the reactor and using a low pressure system between core damage and vessel breach. If cooling is restored within 30 minutes, the probability of successful arrest is assumed to be 1.0, and if cooling is restored after 30 minutes, the probability of successful arrest is assumed to be 0.0. The inclusion of this event in the tree and the assignment of the success path to the Low consequence category are based on the premise that the time window is sufficiently short that minimal in-vessel releases will occur and that they will have a high probability of being scrubbed by the suppression pool, including those from ATWS.

Question 4: No Potential for Early Fatalities?

Early fatalities are largely precluded if an effective evacuation has occurred; only a small fraction of the population is expected to remain behind. Therefore, this question considers the fraction of the remaining core damage frequency (excluding sequences that were arrested as accounted for in the previous question) that involves an effective evacuation. This question allows long-term sequences, such as loss of containment heat removal sequences (TW) or long-term boiloff sequences during shutdown, to be placed in the no "large early release" category without the need for a detailed evaluation of the ultimate containment response. Seismic sequences should all be placed in the potential for early fatality branch on the event tree. Note that to place a sequence on the branch labeled no potential for early fatalities, a licensee should provide information concerning when a general emergency would actually be declared and the expected evacuation time required. For shutdown sequences with the vessel head removed, the time available for evacuation is the time from declaration of a general emergency to the onset of core damage. For other sequences, the time available is the time from declaration of a general emergency to vessel breach. The licensee should use one hour for the time from onset of core damage to vessel breach.

Question 5: RPV Depressurization?

The containment failure probability will be impacted by the RPV pressure at vessel breach. This question addresses the fraction of the remaining core damage frequency (excluding sequences accounted for by previous questions) that are at low versus high pressure. The top branch is the fraction at low pressure, and the bottom branch is the fraction at high pressure.

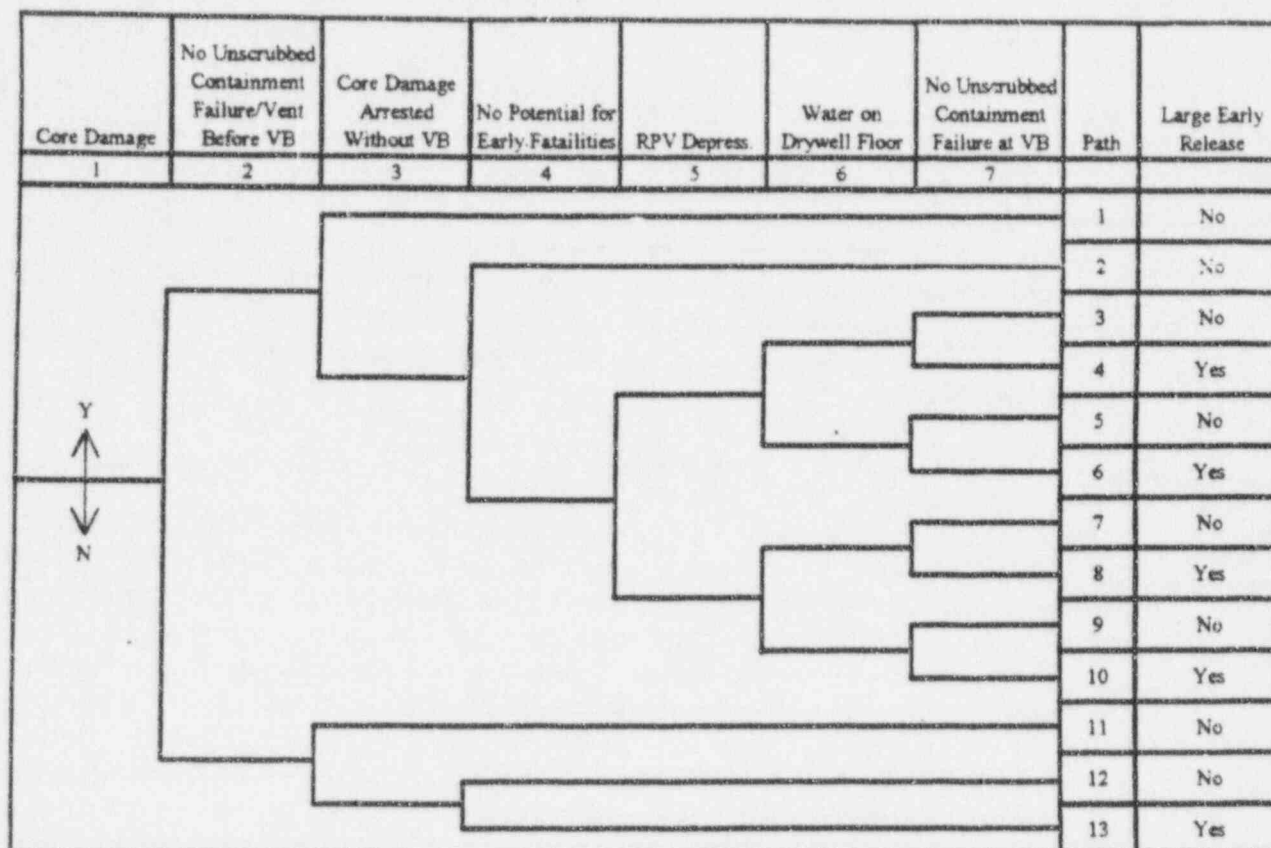


Figure B-3 BWR Mark I Containments

*Note: In the case of seismic initiators, there is a possibility that effective warning and evacuation may be precluded due to the disruption of warning systems and evacuation paths. If the containment structure is predicted to survive the event, the likelihood of long-term containment heat removal should be investigated. If CHR is predicted to fail (for any set of reasons) the containment will eventually fail due to over pressurization and, the consequence category should be "yes" since it is unlikely that evacuation will occur.

It is considered reasonable to use the pressure at the time of core damage, rather than the pressure at vessel breach, if the latter is not readily available. High pressure is considered to be anything above 200 psig in the vessel.

Question 6: Water on the Drywell Floor?

Water in the drywell will affect both the likelihood of ex-vessel steam explosions and the likelihood and consequences of liner meltthrough. Small amounts of water will have limited mitigating effects. It is believed that water levels in excess of 12" will be effective in substantially reducing the probability of meltthrough and/or partially scrubbing the releases. In taking credit for such water, factors, such as the height of the downcomers, pumping capacity, and power availability, must be considered. For this question, the top branch is the fraction of the remaining sequences (excluding sequences accounted for by previous questions) in which at least 12" of water will be available, and the bottom branch is the fraction where 12" of water will not be available.

Question 7: Containment Failure At VB (Releases not scrubbed by suppression pool)?

Depending on the answers to Questions 5 and 6, the containment failure probability is assigned. These failure probabilities implicitly account for the following phenomena: alpha-mode failure, ex-vessel steam explosions, vessel blowdown, liner meltthrough, and direct heating. They do not consider long-term failure modes, such as core-concrete interactions or long-term drywell heatup. Bypass events have been accounted for previously. The branch probabilities for these questions are predetermined (refer to Table B-1 below) and not calculated by the licensee. The licensee could change the probabilities by providing a suitable argument that plant-specific features affect the quantification. The licensee should consider plant-specific features that increase the containment failure and not only those plant-specific features that mitigate severe accidents.

Table B-1. Mark I Conditional Probabilities of Unscrubbed Containment Failure at Vessel Breach

| Path | RPV Pressure | Water | Total Failure Prob |
|------|--------------|-------|--------------------|
| 4 | Lo | Yes | 0.4 |
| 6 | Lo | No | 0.7 |
| 8 | Hi | Yes | 0.6 |
| 10 | Hi | No | 1.0 |

B.5 BWR Mark II Containment

Figure B-4 provides an event tree which allows accident sequences to be allocated to one of two consequence categories for use with PRAs for BWRs with Mark II containments. The structure of the event tree is based on the premise that all early releases that are scrubbed by the suppression pool are sufficiently low that by themselves will not result in individual early fatality risk. Hence, if an early failure occurs with the functionality of the suppression pool intact, it is assumed that the early scrubbed releases will not pose an early fatality threat to the population within one mile of the plant boundary, and that this population will evacuate before substantial core concrete interaction releases or late iodine releases from pools are of a magnitude to cause individual early fatality risk (except in the case of a seismic event, as noted in Figure B-4). Each top event question in the event tree is discussed below. The licensee would be expected to provide the split fractions for all questions with the exception of Question 7.

Question 1: Core Damage Frequency?

This is simply the entry point for the event tree. The frequency for the accident sequence under consideration is entered here.

Question 2: Containment Failed/Vented Prior to Vessel Breach (Releases not scrubbed by suppression pool)?

This question involves the fraction of the core damage frequency where the containment is failed or vented at the start of the accident or prior to vessel failure. Failures at the start of the accident include bypass sequences (Event V), containment isolation failures, and sequences where the containment is initially open. For example, during cold shutdown and refueling, if the containment is open and the vessel head is removed, no credit is given for closing the containment in the presence of the radioactive environment within the containment. Failures after the start of the accident can also occur due to insufficient containment heat removal, e.g., during ATWS or loss of containment heat removal. Loss of containment heat removal accompanied by drywell

Draft for Comment

Appendix B

venting should be put into the "failed" category. Sequences where the only breach of containment integrity prior to vessel failure is through wetwell vents should be put into the "OK" category.

Question 3: Core Damage Arrested Prior to Vessel Failure?

This question accounts for the fact that some sequences may be arrested in-vessel without significant releases from the RPV. All arrested sequences are assigned to the no "large early release" consequence category. Shutdown events where the vessel head has been removed should all be placed in the "Breach" category. Credit for in-vessel arresting of the accident will only be given for cases where recovering AC power will lead to the restoration of ECCS within 30 minutes of the onset of core damage. For example, no credit will be given for an operator manually depressurizing the reactor and using a low pressure system between core damage and vessel breach. If cooling is restored within 30 minutes, the probability of successful arrest is assumed to be 1.0, and if cooling is restored after 30 minutes, the probability of successful arrest is assumed to be 0.0. The inclusion of this event in the tree and the assignment of the success path to the no "large early release" consequence category are based on the premise that the time window is sufficiently short that minimal in-vessel releases will occur and that they will have a high probability of being scrubbed by the suppression pool, including those from ATWS.

Question 4: No Potential for Early Fatalities?

Early fatalities are largely precluded if an effective evacuation has occurred, only a small fraction of the population is expected to remain behind. Therefore, this question considers the fraction of the remaining core damage frequency (excluding sequences that were arrested, as accounted for in the previous question) that involves an effective evacuation. This question allows long-term sequences, such as loss of containment heat removal sequences (TW) or long-term boil off sequences during shutdown, to be placed in the no "large early release" category without the need for a detailed evaluation of the ultimate containment response. Seismic sequences should all be placed in the potential for early fatality branch on the event tree. Note that to place a sequence on the branch labeled no potential for early fatality, a licensee should provide information concerning when a general emergency would actually be declared and the expected evacuation time required. For shutdown sequences with the vessel head removed, the time available for evacuation is the time from declaration of a general emergency to the onset of core damage. For other sequences, the time available is the time from declaration of a general emergency to vessel breach. The licensee should use one hour for the time from onset of core damage to vessel breach.

Question 5: RPV Depressurization?

The containment failure probability will be impacted by the RPV pressure at vessel breach. This question addresses the fraction of the remaining core damage frequency (excluding sequences accounted for by previous questions) that are at low versus high pressure. The top branch is the fraction at low pressure, and the bottom branch is the fraction at high pressure. It is considered reasonable to use the pressure at the time of core damage, rather than the pressure at vessel breach, if the latter is not readily available. High pressure is considered to be anything above 200 psig in the vessel.



*Note: In the case of seismic initiators, there is a possibility that effective warning and evacuation may be precluded due to the disruption of warning systems and evacuation paths. If the containment structure is predicted to survive the event, the likelihood of long-term containment heat removal should be investigated. If CHR is predicted to fail (for any set of reasons) the containment will eventually fail due to over pressurization and, the consequence category should be "yes" category since it is unlikely that evacuation will occur.

Question 6: Water on the Pedestal or Drywell Floor?

Water in the pedestal will affect the likelihood of ex-vessel steam explosions in the pedestal and drain line (and downcomers, when located directly below the vessel). For this question, the top branch is the fraction of the remaining sequences (excluding sequences accounted for by previous questions) in which the pedestal is flooded, and the bottom branch is the fraction where the pedestal is not flooded.

Draft for Comment

Appendix B

Question 7. Containment Failure At Vessel Breach (Unscrubbed by Suppression pool)?

Depending on the answers to Questions 5 and 6, the containment failure probability is assigned. These failure probabilities implicitly account for the following phenomena: alpha-mode failure, ex-vessel steam explosions in-pedestal and drain lines or downcomers), vessel blowdown, and direct heating. These failure probabilities do not include steel shell failure by melt impingement from core debris ejected from the pedestal cavity nor do they include failures in free standing steel shell containments from dynamic loads as a result of ex-vessel steam explosions in the suppression pool that can potentially occur if molten core debris exits the pedestal cavity and enters the pool through the downcomers (this latter failure mode was addressed by the Containment Loads Working Group and is discussed in NUREG-1079¹). Plants that are vulnerable to these failures should modify the failure probabilities, taking into account the plant specific features that contribute to the vulnerability. The failure probabilities also do not consider long-term failure modes, such as core-concrete interactions or long-term drywell heatup. Bypass and events with containment failure or drywell venting have been accounted for previously. The branch probabilities for these questions are predetermined and are not calculated by the licensee. The licensee could change the probabilities by providing a suitable argument that plant-specific features affect the quantification. The licensee should consider plant-specific features that increase the containment failure such as for the steel shelled containment and not only those plant-specific features that mitigate severe accidents.

Table B-2. Mark II Conditional Containment Failure Probabilities

| Path | Pressure | Water | Total Failure Probability |
|------|----------|-------|---------------------------|
| 4 | Lo | Yes | 0.1 |
| 6 | Lo | No | 0.3 |
| 8 | Hi | Yes | 0.3 |
| 10 | Hi | No | 0.3 |

B.6 BWR Mark III Containment

Figure B-5 provides an event tree which allows accident sequences to be allocated to one of two consequence categories for use with PRAs for BWRs with Mark III containments. The structure of the event tree is based on the premise that all early releases that are scrubbed by the suppression pool are sufficiently low that by themselves will not result in individual early fatality risk. Hence, if an early failure occurs with the functionality of the suppression pool intact, it is assumed that the early scrubbed releases will not pose an early fatality threat to the population within one mile of the plant boundary, and that this population will evacuate before substantial core concrete interaction releases or late iodine releases from pools are of a magnitude to cause individual early fatality risk (except in the case of a seismic event, as noted in Figure B-5). Each top event question in the event tree is discussed below. The licensee would be expected to provide the split fractions for all questions with the exception of Question 7.

1 "Estimates of Early Containment Loads from Core Melt Accidents," Draft NUREG-1079, December 1985.

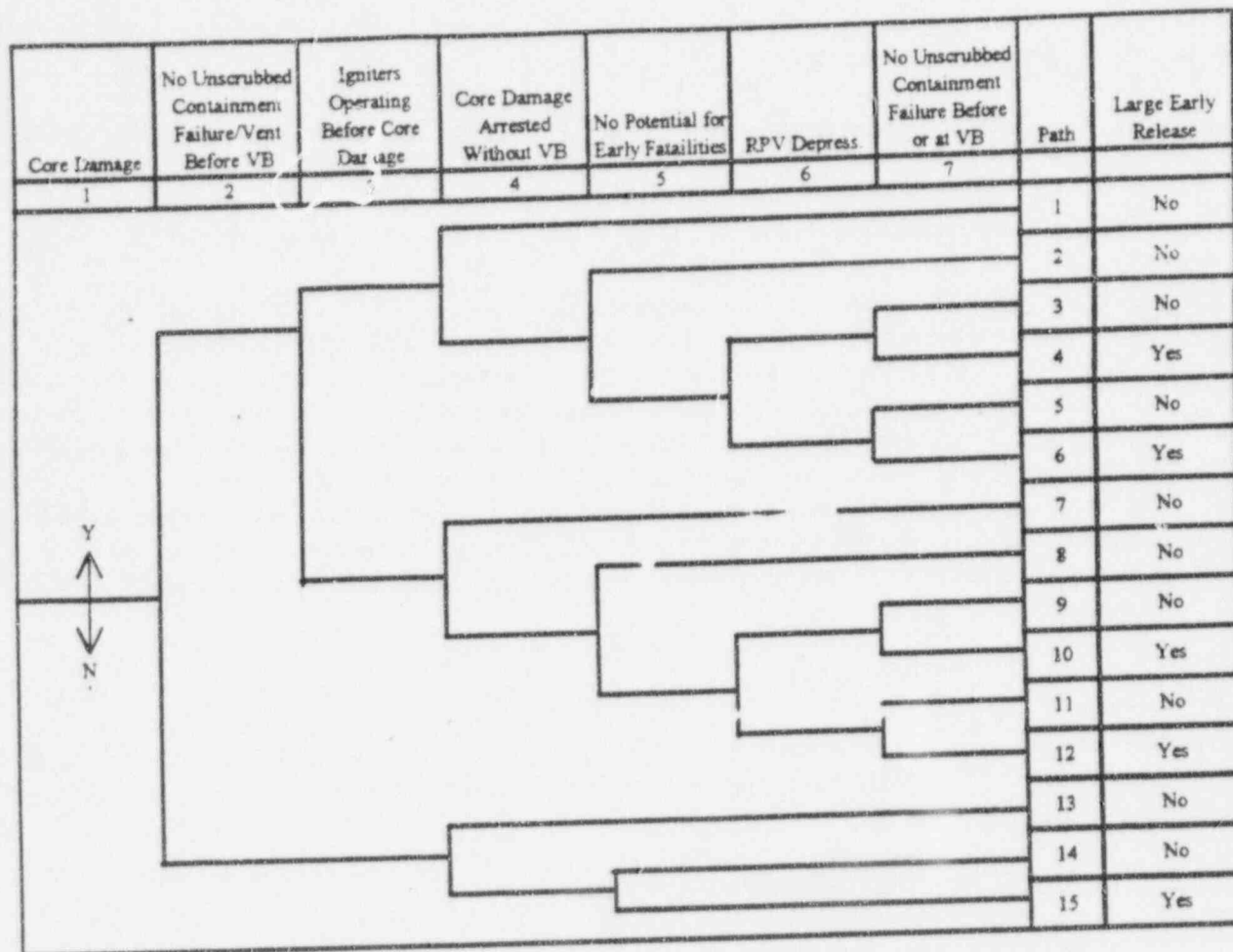


Figure B-5 BWR Mark III Containments

*Note: In the case of seismic initiators, there is a possibility that effective warning and evacuation may be precluded due to the disruption of warning systems and evacuation paths. If the containment structure is predicted to survive the event, the likelihood of long-term containment heat removal should be investigated. If CHR is predicted to fail (for any set of reasons) the containment will eventually fail due to over pressurization and, the consequence category should be "yes" category since it is unlikely that evacuation will occur.

Special Note for Mark III Containments:

Mark III containments essentially have a double layer containment, with the drywell and suppression pool forming one layer and the outer containment structure forming the other layer. In the questions below, the term containment failure refers to containment *functional* failure and requires the following two conditions to *both* be met:

1. The outer containment is breached, and
2. Either the drywell pressure boundary integrity is breached (e.g., by stuck-open drywell vacuum breaker, overpressure failure, or failure to isolate) or the suppression pool drains sufficiently to negate the scrubbing function of the suppression pool.

Draft for Comment

Appendix B

Question 1: Core Damage Frequency?

This is simply the entry point for the event tree. The frequency for the accident sequence under consideration is entered here.

Question 2: Containment Failed/Vented Prior to VB (Releases not scrubbed by suppression pool)?

This question addresses when the containment is failed at the start of the accident or prior to vessel breach (VB). Failures at the start of the accident include bypass sequences (Event V), containment isolation failures, and sequences where the containment is initially open. For example, during cold shutdown and refueling, if the containment is open and the vessel head is removed, no credit is given for closing the containment in the presence of the radioactive environment within the containment. Failures after accident initiation that are addressed here include those due to insufficient containment heat removal, e.g., during ATWS or loss of containment heat removal. Loss of containment heat removal or other non-ATWS sequences where the only breach of containment integrity prior to vessel failure is through wetwell vents should be put into the "OK" category. Containment failure due to uncontrolled hydrogen burns during core damage are considered in Question 7.

Question 3: Hydrogen Igniters Before CD?

This question involves the fraction of the core damage frequency in which the igniters are operating prior to core damage (CD). Nonactuation of the igniters prior to core damage increases the probability of an uncontrolled hydrogen burn.

Question 4: Core Damage Arrested Prior to Vessel Failure?

This question accounts for the fact that some sequences may be arrested in-vessel without significant releases from the RPV. All arrested sequences are assigned to the Low consequence category. Shutdown events where the vessel head has been removed should all be placed in the "Breach" category. Credit for in-vessel arresting of the accident will only be given for cases where recovering AC power will lead to the restoration of ECCS within 30 minutes of the onset of core damage. For example, no credit will be given for an operator manually depressurizing the reactor and using a low pressure system between core damage and vessel breach. If cooling is restored within 30 minutes, the probability of successful arrest is assumed to be 1.0, and if cooling is restored after 30 minutes, the probability of successful arrest is assumed to be 0.0. The inclusion of this event in the tree and the assignment of the success path to the no "large early release" consequence category are based on the premise that the time window is sufficiently short that minimal in-vessel releases will occur and that they will have a high probability of being scrubbed by the suppression pool, including those from ATWS.

Question 5: No Potential for Early Fatalities?

Early fatalities are largely precluded if an effective evacuation has occurred; only a small fraction of the population is expected to remain behind. Therefore, this question considers the fraction of the remaining core damage frequency (excluding sequences that were arrested, as accounted for in the previous question) that involves an effective evacuation. This question allows long-term sequences, such as loss of containment heat removal sequences (TW) or long-term boiloff sequences during shutdown, to be placed in the Low category without the need for a detailed evaluation of the ultimate containment response. Seismic sequences should all be placed in the potential for early fatality branch on the event tree. Note that to place a sequence on the branch labeled no potential for early fatality, a licensee should provide information concerning when a general emergency would actually be declared and the expected evacuation time required. For shutdown sequences

with the vessel head removed, the time available for evacuation is the time from declaration of a general emergency to the onset of core damage. For other sequences, the time available is the time from declaration of a general emergency to vessel breach. The licensee should use one hour for the time from onset of core damage to vessel breach.

Question 6: RPV Depressurization?

The containment failure probability will be impacted by the RPV pressure at vessel breach. This question addresses the fraction of the remaining core damage frequency (excluding sequences accounted for by previous questions) that are at low versus high pressure. The top branch is the fraction at low pressure, and the bottom branch is the fraction at high pressure. It is considered reasonable to use the pressure at the time of core damage, rather than the pressure at vessel breach, if the latter is not readily available. High pressure is considered to be anything above 200 psig in the vessel.

Question 7: Containment Failure Before or At VB (Releases not scrubbed by suppression pool)?

Depending on the answer to Questions 2 and 6, the containment failure probability is assigned. These failure probabilities (refer to Table B-3 below) implicitly account for the following phenomena: hydrogen burns before and at vessel failure, alpha-mode failure, ex-vessel steam explosions, vessel blowdown, and direct heating. They do not consider long-term failure modes, such as core-concrete interactions or long-term pedestal erosion. Bypass events have been accounted for previously. The branch probabilities for these questions are predetermined and are not calculated by the licensee. The licensee could change the probabilities by providing a suitable argument that plant-specific features affect the quantification. The licensee should consider plant-specific features that increase the containment failure and not only those plant-specific features that mitigate severe accidents.

Table B-3. Mark III Conditional Containment Failure Probabilities

| Path | Igniters | Pressure | Total Failure Prob |
|------|----------|----------|--------------------|
| 4 | Yes | Low | 0.2 |
| 6 | Yes | High | 0.2 |
| 10 | No | Low | 0.2 |
| 12 | No | High | 0.3 |

Attachment to Appendix B: Definition of Containment Failure Mode Classes

Early Structural Failure

Involves structure failure of the containment before, during or slightly after reactor vessel failure, usually within a few hours of the start of core damage. A variety of mechanisms can cause early structure failure such as direct contact of the core debris with steel containments, rapid pressure and temperature loads, hydrogen combustion and missiles generated by fuel-coolant interactions.

Containment Bypass

Involves failure of the pressure boundary between the high-pressure reactor coolant system and a low-pressure auxiliary system. For PWRs it can also occur because of the failure of the steam generator tubes, either as an initiating event or as a result of severe accident conditions. In these scenarios, if core damage occurs, a direct path to the environment can exist.

Containment Isolation Failure

Failure to isolate lines that penetrate the containment (the frequency of containment isolation failure includes the frequency of pre-existing unisolable leaks).

Late Structural Failure

Involves structural failure of the containment several hours after reactor vessel failure. A variety of mechanisms can cause late structure failure such as gradual pressure and temperature increases, hydrogen combustion, and basemat melt-through by the core debris.

Containment Venting

Venting is classified as either late or early containment failure depending upon when the vents are opened.



U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

Draft DG-1062

DRAFT REGULATORY GUIDE

DRAFT FOR COMMENT

**An Approach for Plant Specific,
Risk-Informed, Decision Making:**

Inservice Testing

Regulatory Guide DG-1062

March 14, 1997

Contacts: B. Hardin (415-6561), D. Fischer (415-2728)

TABLE OF CONTENTS

| | Page |
|---|------|
| 1 INTRODUCTION | 1-1 |
| 1.1 Background | 1-1 |
| 1.2 Purpose and Scope | 1-3 |
| 1.3 Organization | 1-3 |
| 1.4 Relationship to Other Guidance Documents | 1-4 |
| 1.5 Relationship to the Maintenance Rule | 1-4 |
| 1.6 Relationship to the Proposed Data Rule | 1-4 |
| 2 AN ACCEPTABLE APPROACH TO RISK-INFORMED DECISION MAKING FOR INSERVICE TESTING PROGRAMS | 2-1 |
| 2.1 Key Safety Principles | 2-1 |
| 2.2 A Four-Element Approach to Integrated Decisionmaking | 2-2 |
| 2.2.1 Element 1: Define Proposed Changes to the Inservice Testing Program | 2-2 |
| 2.2.2 Element 2: Conduct Engineering Evaluation | 2-3 |
| 2.2.3 Element 3: Develop Implementation, Performance-Monitoring and Corrective Action Strategies | 2-3 |
| 2.2.4 Element 4: Document Program Proposal | 2-4 |
| 3 ELEMENT 1: DEFINE PROPOSED CHANGES TO INSERVICE TESTING PROGRAM | 3-1 |
| 3.1 Description of Proposed Changes | 3-1 |
| 3.2 Formal Interactions with the Nuclear Regulatory Commission | 3-2 |
| 4 ELEMENT 2: ENGINEERING EVALUATION | 4-1 |
| 4.1 Traditional Engineering Evaluation | 4-1 |
| 4.1.1 Evaluating the Proposed Changes to the Current Licensing Basis | 4-2 |
| 4.1.2 Inservice Testing Program Scope | 4-3 |
| 4.1.3 Inservice Testing Program Changes | 4-6 |
| 4.1.4 Relief Requests and Technical Specification Changes | 4-6 |
| 4.2 Probabilistic Risk Assessment | 4-7 |
| 4.2.1 Probabilistic Risk Assessments for Inservice Testing Applications | 4-9 |
| 4.2.2 Calculating the Risk Increase from Changes in Test Interval | 4-12 |
| 4.2.3 Categorization of Components | 4-14 |
| 4.2.4 Other Technical Issues | 4-14 |
| 4.2.4.1 Initiating Events | 4-15 |
| 4.2.4.2 Dependencies and Common Cause Failures | 4-16 |
| 4.2.4.3 Uncertainty and Sensitivity Analyses | 4-16 |
| 4.2.4.4 Human Reliability Analyses | 4-16 |
| 4.2.4.5 Use of Plant-Specific Data | 4-16 |

TABLE OF CONTENTS - Cont.

| | Page |
|--|---------|
| 4.2.5 Evaluating the Effect of the Proposed Changes on Plant Risk | 4-18 |
| 4.3 Demonstration of Conformance with Key Safety Principles | 4-18 |
| 4.4 Integrated Decision Making | 4-19 |
| 5 ELEMENT 3: IMPLEMENTATION, PERFORMANCE MONITORING, AND CORRECTIVE ACTION STRATEGY | 5-1 |
| 5.1 Program Implementation | 5-1 |
| 5.2 Performance Monitoring | 5-4 |
| 5.3 Feedback and Corrective Action | 5-5 |
| 5.4 Periodic Assessments | 5-7 |
| 6 ELEMENT 4: DOCUMENTATION | 6-1 |
| 6.1 Risk-Informed Inservice Testing Program Plan | 6-1 |
| 6.2 Probabilistic Risk Assessment Records and Supporting Data | 6-1 |
| 6.2.1 Determination and Quantification of Accident Sequences | 6-1 |
| 6.2.2 Initiating Events | 6-2 |
| 6.2.3 Categorization of Inservice Testing Components | 6-2 |
| 6.2.4 Assessment of Proposed Changes | 6-2 |
| 6.2.5 Uncertainty/Sensitivity Analyses | 6-2 |
| 6.2.6 Plant Data | 6-3 |
| 6.3 Integrated Decision Making Process Records | 6-4 |
| 6.4 Performance Monitoring Program | 6-4 |
| 6.5 Feedback and Corrective Action Program | 6-4 |
| 6.6 Implementation Plans and Schedule | 6-5 |
| 7 REFERENCES | 7-1 |

APPENDIX - DETAILED GUIDANCE FOR INTEGRATED DECISION MAKING

FIGURES

| | Page |
|---|------|
| 1 Principles of Risk-Informed Regulation | 2-2 |
| 2 Principal Elements of Risk-Informed Plant-Specific Decisionmaking | 2-5 |

ABBREVIATIONS/DEFINITIONS

| | |
|--------|--|
| SME | American Society of Mechanical Engineers |
| CCF | common cause failure |
| CDF | core damage frequency |
| CLB | current licensing basis |
| EPRI | Electric Power Research Institute |
| FV | Fussell-Vesely risk importance measure |
| GQA | graded quality assurance |
| HEP | human error probability |
| HSSC | high-safety-significant component |
| ISI | inservice inspection |
| IST | inservice testing |
| LERF | containment large release frequency |
| LSSC | low-safety-significant component |
| MCS | minimal cut set |
| NEI | Nuclear Energy Institute |
| NUMARC | Nuclear Utilities Management Research Council |
| O&M | Operations and Maintenance (ASME committee) |
| PRA | probabilistic risk assessment |
| PSA | probabilistic safety assessment |
| RAW | risk achievement worth risk importance measure |
| RI-IST | risk-informed IST (e.g., RI-IST programs) |
| SRP | standard review plan |
| SSC(s) | structures, systems, and components |
| THERP | Technique for Human Error Rate Prediction |
| USAR | Updated Safety Analysis Report |
| USNRC | U.S. Nuclear Regulatory Commission |

DRAFT FOR COMMENT

1. INTRODUCTION

1.1 Background

During the last several years both the U.S. Nuclear Regulatory Commission (NRC) and the nuclear industry have recognized that probabilistic risk assessment (PRA) has evolved to the point where it can be used to a greater extent in supplementing traditional engineering approaches in reactor regulation. After the publication of its policy statement (Reference 1) on the use of PRA in nuclear regulatory activities, the Commission directed the NRC staff to develop a regulatory framework that incorporated risk insights. That framework was articulated in a November 27, 1995, paper to the Commission (Reference 2). This regulatory guide, which addresses inservice testing (IST) and its companion regulatory documents (References 3-11) implement, in part, the Commission policy statement and the staff's framework for incorporating risk insights into the regulation of nuclear power plants.

In 1995 and 1996, the industry developed a number of documents addressing the increased use of PRA in nuclear plant regulation. The American Society of Mechanical Engineers (ASME) published a research guidance document on risk-based IST (Reference 12) and later initiated code cases addressing IST component importance ranking (Reference 13) and testing of certain plant components using risk insights. The Electric Power Research Institute (EPRI) published its "PSA Applications Guide (Reference 14) to provide utilities with guidance on the use of PRA information for both regulatory and non-regulatory applications. The Nuclear Energy Institute (NEI) distributed a draft guideline on risk-based IST (Reference 15) for comment, and then distributed a revised guideline (Reference 16) based on comments received.

1.2 Purpose and Scope

Current IST programs are performed in compliance with the requirements of 10 CFR 50.55a(f) and with Section XI of the ASME Boiler and Pressure Vessel Code which are a part of each plant's current licensing basis (CLB).¹ This regulatory guide describes an acceptable alternative

¹This regulatory guide adopts the 10 CFR Part 54 definition of current licensing basis. That is, "Current Licensing Basis (CLB) is the set of NRC requirements applicable to a specific plant and a licensee's written commitments for ensuring compliance with and operation with in applicable NRC requirements and the plant-specific design basis (including all modifications and additions to such commitments over the life of the licensee) that are docketed and in effect. The CLB includes the NRC regulations contained in 10 CFR Parts 2, 19, 20, 21, 26, 30, 40, 51, 54, 55, 70, 72, 73, 100 and appendices thereto; orders; license conditions; exemptions; and technical specifications. It also includes the plant-specific design-basis information defined in 10 CFR 50.2 as documented in the most recent final safety analysis

DRAFT FOR COMMENT

approach applying risk insights from PRA to make changes to a nuclear power plant's CLB specific to the IST program. An accompanying new Standard Review Plan (SRP) chapter (Reference 9) has been prepared for use by the NRC staff in reviewing RI-IST applications. Another regulatory guidance document, Regulatory Guide DG-1061, "An Approach for Plant-Specific Risk-Informed Decision Making: General Guidance" (Reference 3) is referenced throughout this report. Regulatory Guide DG-1061 provides overall guidance on the technical aspects that are common to developing acceptable risk-informed programs for all applications such as IST (this guide), inservice inspection, graded quality assurance, and technical specifications. Additional information on PRA applications is given in draft NUREG-1602, "A Standard for Probabilistic Risk Assessment (PRA) to Support Risk-Informed Decisionmaking," draft for comment September 27, 1996 (Reference 18). Further information regarding the relationship between this guide, the related SRP chapter, DG-1061, and NUREG-1602 will be given in Section 1.4.

This regulatory guide gives application-specific details on an acceptable method for developing risk-informed IST (RI-IST) programs and supplements the information given in Regulatory Guide DG-1061. It gives guidance on acceptable methods for utilizing PRA information together with established traditional engineering information in the development of RI-IST programs that have improved effectiveness regarding the utilization of plant resources while still maintaining acceptable levels of quality and safety.

In this regulatory guide, an attempt has been made to strike a balance in defining an acceptable process for developing RI-IST programs without being overly prescriptive. Regulatory Guide DG-1061 identifies a list of high-level safety principles that must be maintained during all risk-informed plant design or operational changes. Regulatory Guide DG-1061 and this guide identify acceptable approaches for addressing these basic high-level safety principles, however, licensees may propose alternate approaches for consideration by the NRC staff. It is intended that the approaches presented in this guide be regarded as examples of acceptable practice and that licensees should have some degree of flexibility in satisfying regulatory needs on the basis of their accumulated plant experience and knowledge.

report (FSAR) as required by 10 CFR 50.71 and the licensee's commitments remaining in effect that were made in docketed licensing correspondence such as licensee responses to NRC bulletins, generic letters, and enforcement actions, as well as licensee commitments documented in NRC safety evaluations or licensee event reports."

DRAFT FOR COMMENT

1.3 Organization

This regulatory guide is structured to follow the approach given in Regulatory Guide DG-1061. Chapter 2 gives a brief overview of a four-element process envisioned in the development of an RI-IST program. This process is iterative and generally not sequential. These elements also summarize the NRC review of licensee risk-informed program proposals. Chapter 3 addresses the first element in the process in which the proposed changes to the IST program are described. This description is needed to determine what supporting information is needed and to define how subsequent reviews will be performed. Chapter 4 contains guidance for performing the engineering evaluation needed to support the proposed changes to the IST program (second process element). Chapter 5 addresses program implementation, performance monitoring, and corrective action (third element). Chapter 6 addresses documentation requirements (fourth element) for licensee submittals to the NRC and identifies additional information that should be maintained in the licensee's records in case later review or reference is needed. Chapter 7 contains a list of references, and the appendix contains additional guidance for dealing with certain IST-related issues such as might arise during the deliberations of the licensee in carrying out integrated decision making. Acceptance guidelines are provided throughout the document for the individual topics.

1.4 Relationship to Other Guidance Documents

This regulatory guide gives detailed guidance on an acceptable approach to implement risk-insights in IST programs. This application-specific guide makes extensive reference to draft Regulatory Guide DG-1061.

Companion regulatory guides (References 4-6) address inservice inspection, graded quality assurance, and technical specifications, and contain guidance similar to that given in this RI-IST guide. New SRP chapters associated with each of the risk-informed regulatory guides are given in References 7-11. The SRP sections are intended for staff use during the review of industry requests for risk-informed program changes. SRP Section 3.9.7 (Reference 9) addresses RI-IST and is consistent with the guidance given in this regulatory guide.

References 12-17 give industry guidance for use in developing risk-informed regulatory program changes. These documents have provided useful viewpoints for the staff's consideration during the development of the NRC regulatory guidance documents.

1.5 Relationship to the Maintenance Rule

The Maintenance Rule requires that licensees monitor the performance or condition of structures, systems, or components (SSCs) against licensee-established goals, in a manner sufficient to provide reasonable assurance that such SSCs are capable of fulfilling their intended function. Such goals are to be established, where practicable, commensurate with safety, and are to take into account industrywide operating experience. When the performance or condition of a component does not meet established goals, appropriate corrective actions are to be taken.

Component monitoring that is performed as part of the Maintenance Rule implementation can be used to satisfy monitoring needs for RI-IST, and for such cases, the performance criteria chosen have to be compatible to both the Maintenance Rule requirements/guidance and the RI-IST guidance provided herein. Where a licensee chooses to rely upon its Maintenance Rule monitoring to also satisfy the monitoring needs of its RI-IST program, for safety-related and important to safety SSCs, that monitoring should be subject to the requirements of Appendix B to 10 CFR Part 50.

1.6 Relationship to the Proposed Data Rule

The proposed rule on reporting reliability and availability information for risk-significant systems and equipment (i.e., 10 CFR 50.76, 61 FR 5318) and the associated draft Regulatory Guide DG-1046 (Reference 19) are intended to provide reliability and availability data on selected systems and equipment in U.S. commercial nuclear power plants for use by both the NRC and its licensees. The data would be compiled by the NRC in a centralized database. The definitions and information requested are intended to be sufficient to qualify the database for regulatory applications of probabilistic risk assessment (PRA) that fall within the limitations of the data, e.g., RI-IST programs. Licensees that choose to implement RI-IST programs will be expected to use such plant-specific data, in conjunction with their plant-specific PRA, to help categorize components into the two IST component groups, i.e., low-safety-significant components (LSSCs) and high-safety-significant components (HSSCs). Information gained about the types of failures that occur will also help define the appropriate testing strategies for the two groups of components. In addition, these data will help to improve the accuracy of plant-specific PRA estimates of changes in plant risk projected to result from changes in IST programs.

DRAFT FOR COMMENT

2. AN ACCEPTABLE APPROACH TO RISK-INFORMED DECISION MAKING FOR INSERVICE TESTING PROGRAMS

2.1 Key Safety Principles

Regulatory Guide DG-1061 identifies five key safety principles that must be met for all risk-informed applications and which must be explicitly addressed in risk-informed plant program change applications. As indicated in Regulatory Guide, while these key principles are stated using traditional engineering terminology, efforts should be made, wherever feasible, to utilize risk evaluation techniques to help ensure and to show that these principles are met. These key principles and the location in this guide where each is addressed for RI-IST programs are as follows:

1. *The proposed change meets the current regulations.* [This applies unless the proposed change is explicitly related to a requested exemption or rule change.]
(This principle is addressed in Sections 3.1 and 4.1 of this guide.)
2. *Defense-in-depth is maintained.*
(Section 4.3)
3. *Sufficient safety margins are maintained.*
(Section 4.3)
4. *Proposed increases in risk, and their cumulative effect, are small and do not cause the NRC Safety Goals to be exceeded.*
(Sections 4.2, 4.4)
5. *Performance-based implementation and monitoring strategies are proposed that address uncertainties in analysis models and data and provide for timely feedback and corrective action.*
(Chapter 5)

Regulatory Guide DG-1061 gives additional guidance on the key safety principles applicable to all risk-informed applications. Figure 1 of this guide repeated from Regulatory Guide DG-1061 illustrates the consideration of each of these principles in risk-informed decision making.

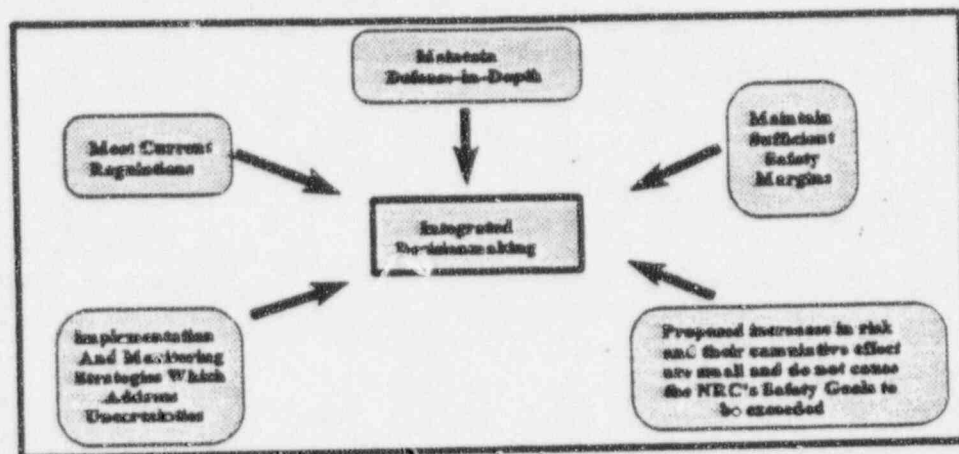


Figure 1 Principles of Risk-Informed Regulation

2.2 A Four-Element Approach To Risk-Informed Decision Making for Inservice Testing Programs

Chapter 2 of Regulatory Guide DG-1061 describes a four-element process for developing risk-informed regulatory changes. An overview of this process specifically related to RI-IST programs is given in this chapter and illustrated in Figure 2. The order in which the elements are performed may vary or occur somewhat in parallel depending on the particular application and the preference of the program developers.

2.2.1 Element 1: Define Proposed Changes to the Inservice Testing Program.

In this element, the licensee should identify the particular components that would be affected by the proposed changes in testing practice. This would include those components currently in the IST program and possibly some that are not if it is determined through new information and insights such as the PRA that these additional components have importance for plant risk. Specific revisions to testing schedules and methods should be described. Plant systems and functions that rely on the affected components should be identified. Chapter 3 gives a more detailed description of Element 1.

DRAFT FOR COMMENT

2.2.2 Element 2: Conduct Engineering Evaluation

In this element, the proposed changes are examined in light of the current plant licensing basis to evaluate the effect of the changes. Areas that are to be evaluated include the expected effect of the proposed RI-IST program on design basis accidents, potential core damage accidents, defense-in-depth attributes and safety margins. Traditional engineering and PRA methods are both used in the evaluation. The results of the two complementary methods are considered together in an integrated decision process that will be carried over into the implementation phase described below in Element 3. During the integration of all of the available information, it is expected that many issues will need to be resolved through the use of a well-reasoned judgement process often involving a combination of different engineering skills. This activity has typically been referred to in industry documents as being performed by an "expert panel." As discussed further at the end of this chapter and in the appendix, this important process is the licensee's responsibility and may be accomplished by means other than a formal panel. In any case, the key safety principles discussed in this guide must be addressed and shown to be satisfied regardless of what approach is used for RI-IST program decision making.

In the planning stages of the program, PRA results may be used to categorize components into LSSC and HSSC groupings. After a plan has been developed, a calculation is made using the plant-specific PRA to evaluate the effect of the planned program changes on the plant risk as measured by core damage frequency (CDF) and containment larger early release frequency (LERF). The risk evaluation should explicitly consider the affected IST components to the extent that it is feasible to model them in the PRA. The necessary scope of the PRA depends upon the particular systems as well as modes of operation that are affected. Regulatory Guide DG-1061 contains extensive guidance regarding the engineering evaluation including acceptance guidelines for projected risk change. Additional application-specific details concerning RI-IST programs and Element 2 are contained in Chapter 4 of this guide.

2.2.3 Element 3: Develop Implementation, Performance-Monitoring, and Corrective Action Strategies.

In this element, plans are formulated that ensure that component reliability is maintained commensurate with the component's safety significance. The planned conditions for operation should be consistent with the assumptions in the PRA analysis to ensure that the PRA results reflect the expected plant behavior. Both testing intervals and methods should be specified, and, to the extent practicable, the testing methods should address the relevant failure mechanisms that could significantly affect component reliability. In the event that component failures occur during the RI-IST program, guidance for evaluating the need for, and the implementation of, corrective

DRAFT FOR COMMENT

action should be included in the plans. Specific guidance for Element 3 is given in Chapter 5.

2.2.4 Element 4: Document Program Proposal

The final element involves preparing that documentation to be included in the submittal and that to be maintained by the licensee for later reference (i.e., archival) if needed. The submittal will be reviewed by the NRC according to the standard review plans given in SRP (NUREG-0800) Chapter 19 and Section 3.9.7 (References 7 and 9 respectively). Documentation requirements for RI-IST programs are given in Chapter 6 of this regulatory guide.

In carrying out this process, the licensee will need to make a number of decisions based on the best available information. Some of this information will be derived from traditional engineering practice and some will be probabilistic in nature resulting from PRA studies. It may be that certain issues discussed in this guide are best evaluated through the use of traditional engineering approaches, but for other issues, PRA may have advantages. It is the licensee's responsibility to ensure that its RI-IST program is developed using a well-reasoned and integrated decision process that considers both forms of input information (traditional engineering and probabilistic) including those cases in which the choice of direction is not obvious. Examples of this latter situation are when there is insufficient information to make a clear decision or if the PRA results appear to disagree with the traditional engineering data. This important decision-making process may at times require the participation of special combinations of licensee expertise (staff) depending on the technical and other issues involved and may at times also have a need for outside consultants. Industry documents have generally referred to the use of an expert panel for such decision making. The appendix to this guide discusses a number of IST-specific issues such as might arise in expert panel deliberations.

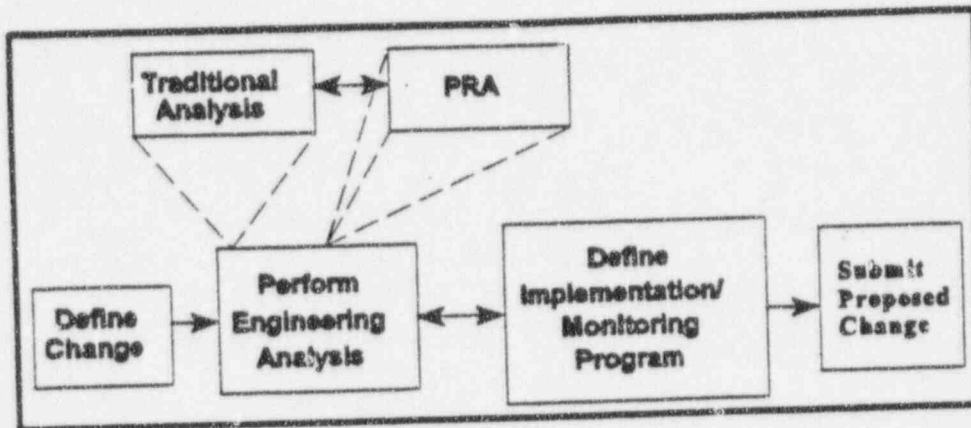


Figure 2 Principal Elements of Risk-Informed, Plant-Specific Decision Making .

DRAFT FOR COMMENT

3. ELEMENT 1: DEFINE PROPOSED CHANGES TO INSERVICE TESTING PROGRAM

In this first element of the process, the proposed changes to the IST program are defined. This involves describing what IST components (e.g., pumps, valves, snubbers) will be involved and how their testing would be changed. Also included in this element is an identification of supporting information, and a proposed plan for the licensee's interactions with the NRC throughout the implementation of the RI-IST.

3.1 Description of Proposed Changes

A full description of the proposed change in the IST program is prepared. This description would include:

- (1) An identification of the aspects of the plant's CLB that would be affected by the proposed RI-IST program. To provide a basis from which to evaluate the proposed changes, the licensee should also confirm that the plant's design and operation is in accordance with its CLB.
- (2) An identification of the specific revisions to existing testing schedules and methods that would result from implementation of the proposed program.
- (3) An identification of the components in the plant's CLB that are both directly and indirectly involved with the proposed testing changes. Any components that are not presently covered in the plant's IST program but are determined to be important to safety (e.g., through PRA insights) should also be identified. In addition, the particular systems that are affected by the proposed changes should be identified since this information is an aid in planning the supporting engineering analyses.
- (4) An identification of the information that will be used in support of the changes. This will include performance data, traditional engineering analyses and PRA information.
- (5) A brief statement describing the way in which the proposed changes meet the objectives of the Commission's PRA Policy Statement.

DRAFT FOR COMMENT

3.2 Formal Interactions With The Nuclear Regulatory Commission

This section gives guidance on the need for licensee reporting of program activities and for formal NRC review of changes made to RI-IST programs.

The licensee can make changes to its approved RI-IST program under the following conditions:

1. Changes made to the NRC-approved RI-IST program that could affect the process and results that were reviewed and approved by the NRC staff (including the change in plant risk associated with the implementation of the RI-IST program) should be evaluated to ensure that the basis for the staff's prior approval has not been compromised. If there is a question regarding this issue, the licensee should seek NRC review and approval prior to implementation.
2. All changes should also be evaluated using the change mechanisms described in existing applicable regulations (e.g., 10 CFR 50.55a, 10 CFR 50.59) to determine if NRC review and approval is required prior to implementation.

For example:

- Changes to component groupings, test intervals, and test methods that do not involve a change to the overall RI-IST approach where the overall RI-IST approach was reviewed and approved by the NRC do not require specific (i.e., additional) review and approval prior to implementation provided that the effect of the changes on plant risk increase is insignificant.
- Component test method changes involving the implementation of an NRC endorsed ASME Code, NRC-endorsed Code Case, or published NRC guidance which were approved as part of the RI-IST program do not require prior NRC approval.
- Test method changes that involve deviation from the NRC-endorsed Code requirements require NRC approval prior to implementation.
- Changes to the RI-IST program that involve programmatic changes (e.g., changes to the plant probabilistic model assumptions, changes to the grouping criteria or figures of merit used to categorize components, and changes in the Acceptance Guidelines used for the licensee's integrated decision-making process) require NRC approval prior to implementation.

DRAFT FOR COMMENT

Component test method changes will typically involve the implementation of an applicable ASME Code or code case (as approved by the NRC) or published NRC guidance. Changes to the component test methods for these situations do not require prior NRC approval. However, test method changes that involve deviation from the NRC approved code requirements do require NRC approval prior to implementation.

The licensee will include in its submittal, a proposed process for determining when formal NRC review and approval are or are not necessary. As discussed, once this process is approved by the NRC, formal NRC review and approval are only needed when the process determines that such a review is necessary, or when changes to the process are requested.

4. ELEMENT 2: ENGINEERING EVALUATION

Overview of Approach

After the proposed change to the licensee's IST program has been defined, the licensee should conduct an engineering evaluation of the proposed change using a combination of traditional engineering methods and PRA. The purpose of this evaluation is to evaluate the proposed change in light of the current licensing basis of the plant to ensure that plant risk is maintained at acceptable levels. The results of this evaluation are to be used in conjunction with the PRA-based information such that the two different approaches complement one another. The major objective of this evaluation is to confirm that the proposed program change will not compromise defense in depth and other key safety principles described in Chapter 2. Regulatory Guide DG-1061 gives general guidance for the performance of this evaluation supplemented by the RI-IST-specific guidance herein.

4.1 Traditional Engineering Evaluation

This part of the evaluation is based on traditional engineering methods (not probabilistic). Areas to be evaluated from this viewpoint include the potential effect of the proposed RI-IST program on design basis accidents, defense-in-depth attributes and safety margins. As indicated above, defense-in-depth and safety margin should also be evaluated, as feasible, using risk techniques (PRA).

4.1.1 Evaluating the Proposed Changes to the Current Licensing Basis

A broad review of the CLB may be necessary. Proposed IST program changes could affect requirements or commitments that are not explicitly stated in the licensee's safety analysis report. Furthermore, staff approval of the design, operation, and maintenance of components at the facility have likely been granted in terms other than probability, consequences, or margin of safety. Therefore, it may be more appropriate to evaluate proposed IST program changes against other more explicit criteria (e.g., criteria used in either the licensing process or to determine the acceptability of component design, operation and maintenance).

Section 50.55a of 10 CFR allows the Director of the Office of Nuclear Regulation to authorize alternatives to the specific requirements of this regulation provided that the proposed alternative will ensure an acceptable level of quality and safety. Thus, alternatives to the examples of

DRAFT FOR COMMENT

acceptable RI-IST approaches presented in this guide may be proposed by licensees so long as supporting information is provided that demonstrates that the key safety principles discussed in Chapter 2 of this guide are maintained.

Acceptance Guidelines

The sources of information for the traditional engineering part of the evaluation should include the IST plan information including component functions from the design-basis documents, references to relevant plant licensing commitments, and approved relief requests. On a component-specific basis, the licensee should identify each instance where the proposed IST program change will affect the CLB of the plant and document the basis for the acceptability of the proposed change by explicitly addressing each of the key safety principles. If the CLB is not affected by the proposed IST program changes, the licensee should indicate this in its RI-IST program description.

4.1.2 Inservice Testing Program Scope

10 CFR 50.55a specifies IST requirements for certain safety-related pumps, valves and snubbers. These components are to be tested according to the requirements of Section XI of the American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code (the Code) or the applicable Operations and Maintenance (O&M) Code. Both Section XI and 10 CFR 50.55a state that the IST program includes certain components classified by the licensee as components which are required to perform a specific function in shutting down a reactor, maintaining the shutdown condition, or mitigating the consequences of an accident.

To ensure that the proposed RI-IST program will provide an acceptable level of quality and safety, the licensee should use the PRA to identify the appropriate scope of components to be included in the program. All of the components that are important to the scope of an RI-IST program must be identified. This will normally include all components that are within the scope of the current IST program. In addition, licensees may identify structures, systems and components (SSCs) with high risk significance which are not currently subject to traditional Code requirements or to a level of regulation which is commensurate with their risk significance. PRA systematically takes credit for non-Code structures, systems and components (SSCs) as providing support, acting as alternatives, and acting as backups to those SSCs that are within the current code. To maintain the validity of the PRA as it is used to categorize components and to evaluate the effect of the proposed RI-IST program on plant risk, the assumptions regarding component

DRAFT FOR COMMENT

reliability and availability must be preserved. Accordingly, these additional risk-important SSCs should be included in licensees' RI-IST proposals. Specifically, the licensee's RI-IST program scope should include those ASME Code Class 1, 2 & 3 and non-Code components that the licensee's integrated decision-making process categorized as HSSCs and thus determined these components to be appropriate additional candidates for the RI-IST program.

To preserve the PRA assumptions which contribute to supporting the proposed RI-IST program, the PRA should also be used to evaluate RI-IST program test requirements (test interval and methods) as well as practicable. Consequently, for the IST components within the scope of the proposed RI-IST program, the licensee should examine the test strategies currently in place to evaluate the test strategy effectiveness, and where appropriate, modify the test strategy.

Acceptance Guidelines

The RI-IST program scope is acceptable if it includes, in addition to components in the current Code prescribed program (i.e., Code class 1, 2, & 3 components), those ASME Code Class 1, 2, & 3 and non-Code components categorized as HSSC. Test strategies should be evaluated to ensure that they are consistent with PRA assumptions.

4.1.3 Inservice Testing Program Changes

This section discusses what licensees need to consider if they propose to change only IST intervals (i.e., if they propose to continue to use the existing approved Code test methods), or if they choose to change both IST intervals and test methods.

Acceptance Guidelines - General

The licensee should reevaluate the IST interval (and methods as applicable) for HSSC components that were the subject of an approved relief request, or an NRC-authorized alternative test. The licensee should resubmit relief requests, and requests that alternatives be authorized, along with risk-related insights, for NRC staff review and approval.

In establishing the test strategy for LSSC components, the licensee should consider component design, service condition, and performance, as well as risk insights. The proposed test interval

DRAFT FOR COMMENT

must be supported by both generic and plant-specific failure rate data and the test interval should be significantly less than the expected time to failure of the SSC in question. The rationale for the proposed change in test interval and its relationship to expected time to failure should be provided. The licensee should ensure that adequate component capability (i.e., margin) exists, above that required during design basis conditions, such that component operating characteristics over time do not result in reaching a point of insufficient margin before the next scheduled test activity. The IST interval should generally not be extended beyond once every 5 years or 3 refueling outages (whichever is longer) without specific compelling documented justification. Extensions beyond 5 years or 3 refueling outages (whichever is longer) will be considered as component performance data at extended intervals is acquired and as PRA technology improves.

IST components (with the exception of check valves) should, as a minimum, be exercised or operated at least once every refueling cycle. If practical, more frequent exercising should be considered for components in any of the following categories:

- i) Components with high-risk significance;
- ii) Components in adverse or harsh environmental conditions; or
- iii) Components with any abnormal characteristics (operational, design, or maintenance conditions).

Licensees choosing to pursue RI-IST programs should consider the adoption of enhanced test strategies developed with ASME risk-based IST Code cases endorsed by the NRC² (or the revised ASME Code after the risk-based Code cases get incorporated into the Code and endorsed by the NRC). Deviations from endorsed Code cases (or revised ASME Code) should be reviewed and approved by the NRC staff via relief requests prior to implementation.

For components that the licensee proposes to place in the HSSC category and that are not in the licensee's current IST program, the following conditions should be met:

These components should be tested in accordance with the ASME Code cases (or revised ASME Code), including compliance with all administrative requirements. Where ASME Section XI or O&M Code testing is not practical, alternative test methods should be developed by the licensee

² Generic letter 96-05, "Periodic Verification of Design-Basis Capability of Safety-Related Motor-Operated Valves," issued September 18, 1996, indicates that risk insights may be used in developing MOV periodic verification programs. It also endorses (with limitations) ASME non-mandatory Code Case OMN-1, entitled: "Alternative Rules for Preservice and Inservice Testing of Certain Electric Motor Operated Valve Assemblies in LWR Power Plants, OM Code 1995 Edition; Subsection ISTC." This code case provides for the use of risk insights in establishing an MOV test program; however detailed guidance is not included. Licensee programs are subject to NRC review.

DRAFT FOR COMMENT

to ensure operational readiness and to detect component degradation (i.e., degradation associated with failure modes identified as being important in the licensee's PRA). As a minimum, a summary of alternative test methods should be reviewed and approved by the NRC as part of this review and prior to implementation of the RI-IST program at the plant.

Acceptance Guidelines - Changes to Test Interval (Only)

If a licensee proposes to only change IST interval (i.e., if the licensee proposes to continue to use the existing approved Code test methods), then the process used by the licensee to categorize components should satisfy the following conditions:

- a) The engineering evaluation should give consideration to components that are potential candidates for decreased component test intervals as well as to candidates for increased intervals.
- b) The effectiveness of the current IST program in determining the capability of the component to carry out its intended function should be assessed. Test intervals should only be extended for components that are tested using methods that have the capability to detect component degradation associated with the important failure modes and causes identified in the plant's PRA.
- c) Extensions to test intervals will be "step-wise."

Acceptance Guidelines - Changes to Test Interval and Method

A process (similar to that described in Reference 16) should be used to develop an appropriate test strategy for IST components. For the HSSC components this should involve the following activities:

- i) a component failure mode and cause analysis ;
- ii) a structured qualitative assessment of the effectiveness of each potential test based on its ability to detect failure, to detect conditions that are precursors to failure, and predict end of service life; and
- iii) a strategy formulation and evaluation for each component taking into account generic and plant-specific performance histories.

DRAFT FOR COMMENT

These tasks may be accomplished through the ASME's IST Code Case (References 13 and 17) as approved by the NRC. If a licensee proposes to change both IST intervals and IST methods, then the process used by the licensee to categorize components should identify components whose test strategy should be more focused as well as components whose test strategy might be relaxed. Extensions to test intervals should be made step-wise.

4.1.4 Relief Requests and Technical Specification Changes

Licensees proposing changes in IST programs based on risk considerations need to address certain issues related to requesting relief from existing program requirements:

Acceptance Guidelines

- Relief is required for any HSSC or LSSC components for which the **test methods** are not in accordance with NRC approved ASME code requirements or NRC guidance.
- Relief is required for any HSSC components for which the **test frequencies** are not in accordance with the approved ASME code requirements or NRC guidance.
- The licensee must submit and have approval of a technical specification amendment prior to implementing the RI-IST program for any components for which there are proposed changes in technical specification requirements.

On a component-specific basis, the licensee should identify each instance where the proposed RI-IST program change is not consistent with the guidance given above. In each such case, the licensee should document the basis for the acceptability of the proposed difference.

4.2 Probabilistic Risk Assessment

Overview of Approach for Probabilistic Evaluations.

Issues specific to the IST risk-informed process are discussed in this section. Regulatory Guide DG-1061 contains much of the general guidance which is applicable for this topic.

The risk-informed application process is intended not only to support relaxation (test interval or method), but also to identify areas in which increased safety resources would be justified. An

DRAFT FOR COMMENT

acceptable RI-IST process should therefore not focus exclusively on areas in which reduced testing could be justified. The increased testing might take the form of a commitment to verify component operability other than through formal IST; for example, credit of this kind might be justified for components whose operability is indirectly and partially verified as a result of IST of other components. This chapter, therefore, addresses IST-specific considerations in the PRA in order to support both relaxation and enhancement of verification of component operability.

The following PRA outputs are generally needed for RI-IST applications :

1. core damage frequency (CDF) and CDF change
2. containment large early release frequency (LERF) and LERF change
3. minimal cut sets (MCS)
4. Fussell-Vesely Importance (FV) and risk achievement worth (RAW) for all SSCs before and after proposed changes, including those from all sensitivity studies

In addition, the FV and RAW importances of all components are required to identify instances in which increased attention (IST or other programs such as technical specifications) might be warranted.

4.2.1 Probabilistic Risk Assessments for Inservice Testing Applications

Quality and Scope of the PRA

For the quantitative results of the PRA to play a major and direct role in decision-making, there is a need to ensure that they are derived from "quality" analyses. Guidance in quality issues for the baseline PRA and for the scope of the PRA is provided by the Regulatory Guide DG-1061.

Level of Detail of the PRA

The development of a RI-IST program will require that plant-specific PRA information be available to identify those IST components that contribute most significantly to the plant's estimated risk. Components covered should include the following:

- Safety-related components that are relied on to remain functional during and after design-basis or beyond design basis events to ensure the integrity of the reactor coolant pressure

DRAFT FOR COMMENT

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 10 CFR Part 100 guidelines.

- non-safety-related components
 - that are relied on to mitigate accidents or transients or are used in plant emergency operating procedures
 - whose failure could prevent safety-related components from fulfilling their safety-related function
 - whose failure could cause a reactor scram or actuation of a safety-related system

Acceptance Guidelines

This issue is addressed acceptably if:

- The PRA quality and scope is acceptable as defined in the general Regulatory Guide DG-1061.
- The components in the proposed RI-IST program are included in the PRA model, or reasons why they are not modeled are justified and documented in terms of the potential effect on the plant's risk.
- All components in the proposed RI-IST program for which credit is taken regarding the plant's accident response capability are shown to be within the scope of programmatic activities (IST, GQA, ISI, maintenance, monitoring).
- The licensee justifies that the proposed RI-IST program will not introduce vulnerabilities or remove from programmatic activities components needed to ensure satisfactory safety performance.

In addition, this guide describes licensee documentation and submittal needs for NRC review.

DRAFT FOR COMMENT

4.2.2 Calculating the Risk Increase from Changes in Test Interval

In order for the PRA to support the decision appropriately, there should be a good functional mapping between the components associated with IST and the PRA basic event probability quantification. Part of the basis for the acceptability of any RI-IST program is a quantitative demonstration by use of a qualified PRA that established risk measures are not significantly increased by the proposed extension in testing intervals for selected components. In order to establish this demonstration, it is necessary that the PRA include models which appropriately account for the change in reliability of the components as a function of testing interval (or test frequency). When feasible, it is also desirable to model the effects of an enhanced testing method. For example, enhanced testing might be shown to improve or maintain component availability, even if the interval is extended. That is, a better test might compensate for a longer interval between tests. Licensees who apply for substantial increases in test interval are expected to address this area, i.e., to proactively seek improvements in testing that would compensate for the increased intervals under consideration.

The following steps should be performed:

- (1) identification of all RI-IST systems, and components
- (2) identification of all affected cut-sets and RI-IST-related basic events
- (3) review of the model used to quantify each affected basic event. Most fundamentally, the process should consider the effect of test strategy (interval and method) on unavailability

A check should also be performed to determine if non-IST manipulation has been credited either in IST basic events or in compensating-component basic events. If a component is stroked or challenged between instances of IST, and if these activities are actually capable of forcing recognition of a component failure, then the effective fault exposure time is indeed less than the RI-IST interval. It can be appropriate to take credit for this effective shortening of fault exposure time in the PRA quantification, provided that there is assurance that the important failure modes are in fact identified by the stroking or the system challenges. This is not always trivial: if a functional success can be achieved by any one of n components in parallel, so that the function succeeds even if $n-1$ of the components fail, then merely monitoring successful functional response does not show whether all components are good, unless proactive verification of each component's state is undertaken. In addition to this, some instances of revealing a component fault through challenge have adverse consequences, including functional failure, and if credit is taken for shortening fault exposure time through functional challenges, then it is necessary to account for this downside in the quantification of accident frequency.

DRAFT FOR COMMENT

Modeling Increases In Test Interval

The relationship between the component unavailability on demand, q , and the test interval is usually approximated by:

$$q = \frac{1}{2} \lambda T$$

where:

λ is the failure rate, and

T is the time interval between tests.

In addition to transitions to a failed state that occur between component demands or tests, there is also a "demand-related" contribution to unavailability, corresponding to the probability that a component will fail to operate when demanded, even though for some purposes it would have been considered "good" before being subjected to the stress of the demand itself. This would have the effect of adding a constant to the test-interval-dependent contribution to q identified above. The assumption that the total q scales linearly with the test interval (i.e., doubles when test interval doubles) is "conservative" in the sense that it scales the test-interval-independent contribution along with the test-interval-dependent contribution, and in that respect tends to overstate the effect of test interval extension. This approximation is therefore considered acceptable; however, it should be noted that guidance aimed at improving the capability of tests to identify loss of performance margin is aimed partly at reducing the "demand" contribution as well, so that improved modelling in this area would appear to have the potential to support further improvements in allocation of safety resources.

As test intervals are extended, there is some concern that the failure rate, λ , may increase. This failure rate, generally assumed constant, is based on data from current IST test intervals, and therefore does not include effects which may arise from extended test intervals. It is possible that insidious effects such as corrosion or erosion, intrusion of foreign material into working parts, adverse environmental exposure, breakdown of lubrication, etc. which have not been encountered with the current shorter test intervals could significantly degrade the component if test intervals become excessively long. One way to address this uncertainty is to use the PRA insights to help to design an appropriate implementation and monitoring program, for example, to approach the interval increase in a stepwise fashion rather than going to the theoretically-allowable maximum in a single step, or to stagger the testing of redundant components (test different trains on alternating schedules) so that the population of components is being sampled relatively frequently, even though individual members of the population are not. By using such approaches, the

DRAFT FOR COMMENT

existence of the above effects can be detected and compensatory measures taken to correct the testing of the remaining population members. However, it is important that the monitoring includes enough tests to be relevant, and that the tests are capable of detecting the time related degradation (performance monitoring is discussed in Section 5.2).

Modeling Enhanced Testing Procedures

In addition to the issues raised by leaving components untested for longer periods, there is also the issue of test effectiveness. Licensees are encouraged to employ enhanced testing techniques to improve detection of degraded and failed components. All licensees proposing to extend testing intervals should also address test effectiveness. This includes both conscious effort to improve testing according to state of the art guidance, and, for licensees who wish to invoke credit for detecting degraded components, improvements in reliability modelling of basic event probability as a function of testing policy.

Acceptance Guidelines

- The PRA should include a model which provides an appropriate measure of the risk significance of extending the test interval on selected components. This requires that the model directly addresses the change in component availability as a function of test interval. The analysis should include:
 - an explicit quantitative consideration of the degradation of the component failure rate as a function of time, supported by appropriate data and analysis,
- OR
- arguments which support the conclusion that no significant degradation will occur.
- The model should consider the effects of enhanced testing to the extent practicable. If the application seeks a substantial increase in interval, then a proactive search for compensating improvements in testing should be made. If the testing is shown to be already as effective as can be expected, then an absolute requirement for test improvement should not be imposed. However, an evaluation should be made to determine whether any common cause group is slated for a major extension of test interval, and if so, whether there is any way that enhanced testing could address common cause potential.

DRAFT FOR COMMENT

If credit for enhanced testing was taken, the model should treat it explicitly.

4.2.3 Categorization of Components

General guidelines for risk categorization of components using importance measures and other information are provided in Regulatory Guide DG-1061. These general guidelines address acceptable methods for carrying out categorization and some of the limitations of this process. Guidelines that are specific to the IST application are given in this section. As used here, risk categorization refers to the process for grouping IST components into LSSC and HSSC categories.

As indicated, risk importance results from the PRA may be used as one of the inputs to the categorization process. Unfortunately, many components of interest to RI-IST are often not included in existing PRA models, and so there is no quantified risk importance information for these components. When feasible, adding these components to the PRA should be considered by the licensee. In cases where this is not feasible, information based on traditional engineering analyses and judgement must be used to determine if a component should be treated as LSSC or HSSC.

The identification of components for a change in IST intervals or test methods can be done using different methods. Component categorization by use of PRA importance measures to classify components into HSSC and LSSC categories is one method. Categorization or component grouping may also be accomplished using more traditional engineering approaches with data developed from operating experience.

In addition to component categorization efforts, the determination of safety significance of components by the use of PRA-determined importance measures is important for several other reasons:

- When performed with a series of sensitivity evaluations, it can identify potential risk outliers by identifying IST components which could dominate risk for various plant configurations and operational modes, PRA model assumptions, and data and model uncertainties.
- Importance measure evaluations can provide a useful means to identify improvements to current IST practices during the risk-informed application process.

DRAFT FOR COMMENT

- System level importance results can provide a high level verification of component level results and can provide guidance for the ranking of IST components that are not modeled in the PRA.

While categorization is an essential step in defining how the RI-IST will be implemented, it is not an essential part of ensuring the maintainance of an acceptable level of plant risk. As described in Section 4.2.5, the sensitivity of risk importance measures to changes in IST strategy (i.e., proposed for RI-IST) can be used as one input to overall understanding of the effect of this strategy on plant risk. However, the traditional engineering evaluation described in Section 4.1 and the calculation of change in overall plant risk described in Section 4.2.5 provide the major input to the determination of whether the risk change is acceptable or not.

Acceptance Guidelines

When using risk importance measures to identify high and low safety significant components, potential limitations of these measures have to be addressed. Variations (including uncertainties) in PRA modeling techniques, assumptions, and data could have a significant impact on the results of the component categorizations using importance measures. Sensitivity studies and/or other evaluations have to be carried out to ensure that changes in risk importance categorizations due to these effects do not result in RI-IST programs that have unacceptable levels of plant risk. Issues that have to be considered and addressed when determining low safety significance of components include: truncation limits; different risk metrics; multiple component importances; consideration of all allowable plant configurations; sensitivity analysis for common cause failures; and sensitivity analysis for recovery actions. These issues are discussed more in detail in Regulatory Guide DG-1061.

In addition to results from PRA importance measures (and the associated sensitivity studies), IST components should also be categorized based on traditional engineering considerations and on plant-specific operational characteristics.

DRAFT FOR COMMENT

4.2.4 Other Technical Issues

4.2.4.1 Initiating Events

For purposes of determining RI-IST requirements, all initiating events (internal and external) and all operating modes should be evaluated to see whether initiating events and predicted plant response are affected by RI-IST proposed changes. At a minimum, all internal event initiators that have been evaluated in the PRA and all external event initiators that have been shown to contribute to the upper 95 percent of the total CDF have to be included in the IST risk determination process. In addition, other initiators including those that have been screened out (eliminated) from the base PRA have to be considered by answering the following questions.

- (1) Does the IST issue involve a change that could lead to an increase in the frequency of a particular initiator already included in the PRA?
- (2) Does the IST issue involve a change that could lead to an increase in the frequency of a particular initiator initially screened out of the PRA?
- (3) Does the IST issue affect the quantification of previously identified accident scenarios for specific initiators that were screened out and eliminated from the PRA because of truncation?
- (4) Does the IST issue affect only specific initiators?
- (5) Does the IST issue have the potential to introduce a new initiating event?

Acceptance Guidelines

- (1) The impact of the proposed plant change on the potential for event initiators (internal and external) already included in the PRA should be determined. For example, less frequent testing could lead to an increase in the frequency of transients for the loss-of-feedwater or loss of support systems. The initiators included in an evaluation should include any initiators for which the plant change directly affects the frequency of the initiating event.
- (2) The impact of the plant change on the frequency of an initiating event originally identified in the PRA but screened due to low frequency should be determined. For example, if less frequent pump and valve testing could lead to an increase in the frequency of loss-of-

DRAFT FOR COMMENT

coolant-accident (LOCA) initiators that were initially screened from an analysis of a shutdown plant operational state (POS), then the impact of such an increase in LOCA frequency should be reexamined.

- (3) The impact of the plant change on the failure rates of SSCs already included in a risk analysis should be considered. SSCs that show a change in their failure probability as a result of the plant change should be addressed in the analysis. Therefore, initiators which depend on the affected SSCs to achieve safe shutdown and that were initially eliminated from the PRA should be reexamined.
- (4) If the regulatory issue affects only specific initiators, then only those specific initiators should be reexamined. For example, if the issue results in changes only to the fire barrier failure probabilities, then only those initiators important to fire risk will have to be reexamined.
- (5) The effect of an IST program change should be examined to determine whether it could introduce a new initiating event. If so, then its effect should be included in the PRA.

4.2.4.2 Dependencies and Common Cause Failures

The effects of dependencies and Common Cause Failures (CCFs) for IST components need to be considered carefully because of the significance they can have on core damage frequency. Generally, data are insufficient to produce plant-specific estimates based solely on the data. For CCFs, data from generic sources may be required.

Acceptance Guidelines

- For those components for which CCF contributions are not included in the PRA models and this exclusion is justified on the basis of historical and engineering evidence driven by current IST requirements, there would be no assurance that the CCF contribution would not become significant under the new proposed IST requirements. Therefore, this issue has to be addressed either using sensitivity studies or as part of a qualitative assessment.
- For RI-IST applications, the potential for cross system CCFs should be investigated. Guidance for performing such evaluations is given in Regulatory Guide DG-1061.

DRAFT FOR COMMENT

4.2.4.3 Uncertainty and Sensitivity Analyses

Uncertainty and sensitivity analyses are expected to play an important (and complex) part in the support of risk-informed IST program changes. The current guidance on these topics is given in Regulatory Guide DG-1061. It is expected that certain application-specific guidance will be developed from the ongoing NRC reviews of the proposed RI-IST pilot plant programs.

4.2.4.4 Human Reliability Analyses

Guidance on this topic is given in Regulatory Guide DG-1061. Some IST-specific guidance follows.

Acceptance Guidelines

- The technique(s) used to identify and quantify human actions should be such that they take into account the performance-shaping (or performance-influencing) factors that are applicable for IST-related events.
- The effects of innovative recovery actions that are modeled in the PRA should be considered to determine how component ranking can be affected. The concern here stems from situations in which very high success probabilities are assigned to recovery events for certain sequences, thereby resulting in related components being risk insignificant. Furthermore, the ranking of SSCs should not be affected by recovery actions that are only modeled for limited scenarios. Sensitivity analyses should be used to assess the impact of variations in the probability of failure to recover.

4.2.4.5 Use of Plant-Specific Data

In selecting appropriate failure rate data to use in the RI-IST program for the IST components, 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. 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.

DRAFT FOR COMMENT

As extended test intervals are 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 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. Poor performance may arise because of inherent characteristics of one member of what would otherwise be considered a uniform population. This would result in a higher than expected failure rate for the population and lead to less relaxation than might be anticipated. Of more concern is poor performance of components that arises because they are operating in a more demanding environment for example. If, for reasons of expediency, these components are grouped together with others for which the operating conditions are more favorable, then their failure rates could become artificially lowered, and, if requirements are relaxed based on the group failure rate, this could lead to a significant probability of experiencing an in-service failure of one of these poor performers.

Acceptance Guidelines

- 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. For those licensees who propose to use plant specific data only, the data should be justified.
- 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 the testing scheme (interval and methods) would be considered adequate to support the performance credited to them in the risk analysis, based on a component-specific failure rate consistent with the number of failures experienced. Section 5.3 of this guide discusses feedback and corrective action.

DRAFT FOR COMMENT

4.2.5 Evaluating the Effects of the Proposed Changes on Plant Risk

An assessment of the overall or cumulative effect of all proposed changes in plant design and operation on plant risk is critical to determining the acceptability of the changes. This guide addresses acceptable methods for assessing risk changes associated with IST program changes, however, if changes in graded quality assurance or technical specifications are also being considered, the integrated effects of all of these proposed activities should be evaluated.

Licensees should not assume a low failure rate in one application, e.g., IST, then reduce quality assurance of components included in the IST program (possibly negating the assumed low failure rate) without providing justification. It is possible that more frequent testing (RI-IST) could compensate for a reduction in quality assurance or maintenance provided, again, that supporting analysis and documentation is included in a licensee's submittal.

Acceptance Guidelines

See Section 2.4.2 of Regulatory Guide DG-1061 for more extensive guidance on this subject.

4.3 Demonstration of Conformance with Key Safety Principles

Section 2.1 of this guide indicates specific sections of the guide that address each of the key safety principles including acceptance guidelines. Two of the more difficult areas are those involving consideration of defense in depth and safety margin. These are addressed in this section to identify the major areas to be considered consistent with Regulatory Guide DG-1061. More application specific guidance will be added after the staff gains more experience from the review of the IST pilot plant programs.

Defense-in-depth evaluation

As stated in Regulatory Guide DG-1061, general design criteria, national standards and engineering principles such as the single failure criterion are to be considered. Assurance that this criterion is met is when:

- the PRA shows that there is preserved a reasonable balance between core damage prevention, prevention of containment failure, and consequence mitigation,

DRAFT FOR COMMENT

- there is not an over-reliance on programmatic activities to compensate for plant design weaknesses,
- system redundancy, independence and diversity are maintained commensurate with the expected frequency and consequences of challenges to the system,
- defenses against potential common cause failures are maintained, and the introduction of new common cause failure mechanisms is avoided,
- independence of barriers is not degraded, and
- defenses against human errors are maintained

Safety margin evaluation

Assurance that this criterion is met is mainly demonstrated by showing that the codes and standards or alternatives approved for use by the NRC that are associated with IST and discussed in Section 4.1 are met. The second means for demonstrating sufficient safety margin is a review of the safety analysis acceptance criteria in the CLB (e.g., updated safety analysis report (USAR), supporting analyses) showing that these criteria are still met for the proposed RI-IST program, or that sufficient margin exists to account for analysis and data uncertainty.

4.4 Integrated Decision Making

This section discusses the integration of all of the technical considerations involved in reviewing submittals from licensees proposing to implement RI-IST programs. General guidance for risk-informed applications is given Regulatory Guide DG-1061 (Reference 3) and in the new SRP sections, Chapter 19 (Reference 7) for general guidance, and Section 3.9.7 (Reference 9) for IST programs. These documents discuss a set of regulatory findings that form the basis for the staff's writing an acceptable safety evaluation report (SER) for a licensee's risk-informed application. Specifically, Section 2.1 of Regulatory Guide DG-1061 identifies a set of "expectations" that licensees should follow in addressing the key safety principles. Due to the importance of these findings, certain of them will be repeated here.

DRAFT FOR COMMENT

Necessary Findings

- The comprehensive plant model, including the PRA and the associated deterministic analysis, is technically sound and supports the rest of the findings regarding the proposed RI-IST program. The analysis is based on the as-built and as-operated and maintained plant.
- All safety impacts of the proposed changes to the licensee's IST program have been evaluated in an integrated manner as part of an overall risk management approach in which the licensee is using risk analysis to improve operational and engineering decisions broadly and not just to eliminate requirements he sees as undesirable. The approach used to identify changes in requirements for IST were used to identify areas where requirements in IST should be increased as well as reduced.
- The acceptability of the proposed changes to the licensee's IST program have been evaluated by the licensee in an integrated fashion that ensures that all of the key safety principles are met.
- The cumulative risk evaluation accounting for all of the proposed IST program changes confirms that changes to the plant core damage frequency (CDF) and large early release frequency (LERF) are small in conformance with the guidelines given in Section 2.4.2.1 of Regulatory Guide DG-1061.
- Appropriate consideration was given to uncertainty in the analyses and interpretation of the results.
- Certain qualitative and defense-in-depth evaluations have been performed, and insights from these have been duly incorporated into the classification scheme, the performance goals, and the associated programmatic activities. These evaluations confirm that sufficient safety margins and defense in depth are maintained.
- The licensee's proposal was subjected to quality controls including an independent peer review.
- Pumps, valves, snubbers and operator actions have been identified and appropriately classified for use in prioritizing and implementing the program. In particular, important components not modeled in the PRA have been identified and appropriately classified utilizing available deterministic supporting information.

DRAFT FOR COMMENT

- After the RI-IST program is approved and initiated, plant performance is supported by testing and analysis and maintained by programmatic activities goals by comparison against specific performance criteria.
- The data, analysis methods and assessment criteria used in the development of the RI-IST are scrutable and available for public review.

These findings are seen to comprise both probabilistic and traditional engineering considerations, which are addressed in more detail in this chapter and in Regulatory Guide DG-1061.

Licensees are expected to review commitments related to outage planning and control to verify that they are appropriately reflected in the licensee's component grouping. Licensees should verify that IST components that play an integral role in the licensee's plans and procedures for maintaining the key shutdown safety functions identified in NUMARC 91-06 are in the high safety significant component group. This should include components required to maintain adequate defense in depth as well as components that might be operated as a result of contingency plans developed to support the outage.

Licensees are also expected to review licensing basis documentation to ensure that the traditional engineering related factors mentioned above are adequately modeled or otherwise addressed in the PRA analysis.

When making final programmatic decisions, choices must be made based on all of the available information. There may be cases where information is incomplete or where conflicts appear to exist between the traditional engineering data and the PRA-generated information. It is the responsibility of the licensee in such cases to ensure that well-reasoned judgement is used to resolve the issues in the best manner possible including due consideration to the safety of the plant. This process of integrated decision making has been discussed in various industry documents (References 14 through 19) with reference to the use of an "expert panel." The appendix to this regulatory guide includes some detailed guidance on certain aspects of integrated decision making specific to RI-IST programs. As discussed in the appendix, it is not intended to specify that an administrative body such as an expert panel must be always formed by the licensee to fulfill this function. Following below are some general acceptance guidelines for this important activity with more specific details given in the appendix.

In summary, acceptability of the proposed change should be determined using an integrated decision-making process that addresses three major areas: (1) an evaluation of the proposed change in light of the plant's current licensing basis, (2) an evaluation of the proposed change

DRAFT FOR COMMENT

relative to the key principles and the acceptance criteria, and (3) the proposed plans for implementation, performance monitoring, and corrective action. As stated in the Commission's Policy Statement on the increased use of PRA in regulatory matters, the PRA information used to support the RI-IST program should be as realistic as possible, with reduced unnecessary conservatism yet including a consideration of uncertainties. These factors are very important when considering the cumulative plant risk and accounting for possible risk increases as well as risk benefits. The licensee should carefully document all of these kinds of considerations in the RI-IST program description including those areas that have been quantified through the use of PRA as well as qualitative arguments for those areas that cannot be readily quantified.

Acceptance Guidelines

- The licensee's proposed RI-IST program should be supported by both a traditional engineering analysis and a PRA analysis.
- The licensee's RI-IST program submittal should be consistent with the acceptance guidelines contained throughout this regulatory guide, specifically with the findings listed in this section, or justify why an alternative approach is acceptable.
- If the licensee's proposed RI-IST program is acceptable based on both the deterministic and probabilistic analyses, it may be concluded that the proposed RI-IST program provides "an acceptable level of quality and safety" [ref. 10 CFR 50.55a (a)(3)(i)].

5. ELEMENT 3: IMPLEMENTATION, PERFORMANCE MONITORING, AND CORRECTIVE ACTION STRATEGIES

Upon approval of an RI-IST program, the licensee should have in place an implementation schedule for testing all HSSCs and LSSCs identified in their program. This schedule should include test strategies and testing frequencies for HSSCs and LSSCs that are within the scope of the licensee's IST program and components identified as HSSCs that are not currently in the IST program.

5.1 Program Implementation

The current ASME Code requires that all safety-related components within the program scope as defined in the applicable ASME Code be tested on a quarterly frequency regardless of safety significance. The authorization of a risk-informed inservice testing program will allow the extension of certain component testing intervals and modification of certain component testing methods based on the determination of individual component importance. The implementation of an authorized program will involve scheduling test intervals based on the results of probabilistic analysis and deterministic evaluation of each individual component.

The RI-IST program should distinguish between LSSCs and HSSCs for testing intervals. Components that are being tested using specific ASME Codes, NRC-endorsed Code cases for RI-IST programs, or other applicable guidance should be individually identified in the RI-IST program. The test intervals of the HSSCs should be included in the RI-IST program for verification of compliance with the ASME Code requirements and applicable NRC-endorsed ASME code cases. Any component test interval or method which is not in conformance with the above should have an approved relief request for that component. Plant corrective action and feedback programs (see Section .) should be appropriately referenced in the IST program and implementing and test procedures to ensure that testing failures are fed back to the plant expert panel and IST coordinator for reevaluation and possible adjustment to the component's grouping and test strategy.

It is acceptable to implement RI-IST programs on a phased approach. Implementation of interval extension for LSSCs may begin at the discretion of the licensee. Implementation may take place on a component, train or system level because extension of the test interval for these components (i.e., either individually or as a group) will have already been demonstrated through PRA and associated sensitivity analysis to have a minimal impact on the figures of merit. However, it is not acceptable to immediately adjust the test intervals of LSSCs to the maximum testing interval

DRAFT FOR COMMENT

allowed by the PRA analysis unless component performance has demonstrated significant reliability or that aging is not an issue. Normally, test interval increases will be done step-wise with gradual extensions being permitted consistent with cumulative performance data for operation at the extended intervals. The licensee will be required to submit the actual testing intervals with their RI-IST program submittal.

For HSSCs, if the licensee initially chooses not to implement any of the ASME Code cases directed at providing alternative test strategies for RI-IST programs (when endorsed by the NRC staff), then testing will be conducted at the required Code interval. Otherwise, the implementation phase of the RI-IST program will be predominantly guided by ASME Code cases. Implementation may take place on a component, train, or system level as allowed in the Code case.

For components that the licensee proposes to place in the HSSC group that are not in the current IST program, the following conditions should be applied:

These components should be inservice tested commensurate with their safety significance. Where ASME Section XI or O&M testing is practical, these components should be tested in accordance with the ASME Code, including compliance with all administrative requirements. Where ASME Section XI or O&M testing is not practical, alternative test methods should be developed by the licensee to ensure operational readiness and to detect component degradation (i.e., degradation associated with failure modes identified as being important in the licensee's PRA). As a minimum, a summary of alternative test methods should be reviewed and approved by the NRC as part of this review and prior to implementation of the risk-informed IST program at the plant. This is consistent with previous NRC practice.

A majority of components contained within plant IST programs are exercised or operated for reasons other than inservice testing such as during normal plant operations and as a result of other component inservice testing. The remaining components are exercised only during IST. An exercise of a component as part of a system test or normal operations does not constitute an inservice test because it provides little or no information on component degradation. However, depending on the system test or plant activity and the extent that the component is exercised, assurance can be gained that the component operated at the time of the test. While this provides little or no information on component degradation, it does provide some assurance that any degradation that may have occurred was not significant enough to degrade the system function.

An acceptable method to extend the test interval for LSSCs that are exercised as a result of plant operations and other testing is to group like components (e.g., NRC Generic Letter 89-04, Position 2 for check valves) and stagger their testing equally over the interval identified for a

DRAFT FOR COMMENT

operations and other testing is to group like components (e.g., NRC Generic Letter 89-04, Position 2 for check valves) and stagger their testing equally over the interval identified for a specific component based on the probabilistic analysis and deterministic evaluation of each individual component. Component grouping should also consider valve actuator type for power operated valves and pump driver type, as applicable. With this method, generic age-related failures can potentially be identified while allowing immediate implementation for some components. LSSCs which are exercised only during RI-IST should have their intervals extended by gradually stepping out the current and successive test intervals until the proposed extended test interval established by the licensee in their engineering evaluation is attained. Then, these low LSSCs should be tested on a staggered basis. The selected test frequency for LSSCs that are to be tested on a staggered basis should be justified in the RI-IST program.

Acceptance Guidelines

For either HSSCs or LSSCs that will be tested in accordance with the current Code test interval and method requirements, no specific implementation schedule is necessary. The test interval should be included in the licensee's RI-IST program.

For either HSSCs or LSSCs that will employ NRC-endorsed ASME Code cases, implementation of the revised test strategies should be documented in the licensee's RI-IST program.

For any alternate test strategies proposed by the licensee, the licensee should submit a relief request to the NRC as discussed in Section 4.1.4 of this guide.

The licensee may group and test LSSCs, which are exercised as a result of plant operation or testing of other components, on a staggered and extended interval basis provided that they have acceptable performance histories. Grouping is acceptable provided it complies, for example, with the guidance contained in NRC Generic Letter 89-04, Position 2 for check valves; Supplement 6 to NRC Generic Letter 89-10 and Section 3.5 of ASME Code Case OMN-1 for motor operated valves.

Component monitoring that is performed as part of the Maintenance Rule implementation can be used to satisfy monitoring as described in the RI-IST program guidance. In these cases, the performance criteria chosen have to be compatible with the RI-IST guidance provided in this guide.

DRAFT FOR COMMENT

For LSSCs that will be tested at an interval greater than the Code test interval, which are not exercised as a result of plant operation or testing of other components, the licensee should increase the test interval successively in a step-wise manner until the components are tested at the maximum proposed test interval provided these components have acceptable performance histories. If no age-dependent failures occur, then the test interval can be gradually extended until the component, or group of components if tested on a staggered basis, is tested at the maximum proposed extended test interval.

5.2 Performance Monitoring

The purpose of performance monitoring is to help confirm that the failure rates assumed for this equipment remain valid, and that no insidious failure mechanisms which are related to extended test intervals become important enough to alter the failure rate assumed in the PRA models. The important criteria must be measurable and the test frequency must be sufficient to provide meaningful data. In addition, the testing procedures and analysis must provide assurance that performance degradation is detected with sufficient margin that there is no adverse effect on public health and safety (i.e., the failure rates cannot be allowed to rise to unacceptable levels before detection and corrective action take place).

A performance monitoring program should be included as part of the licensee's RI-IST program if extending the test intervals for LSSCs is proposed. This program must provide assurance that components placed on the extended test interval will continue to perform as assumed in the PRA, and that any performance degradation is detected and corrected before the extended test program is fully implemented. The program should also include monitoring similar component performance at other plants to establish a sufficient data base of temporal related degradation. Testing procedures should detect degradation in component performance and ideally would replicate, as much as practical, actual demand conditions.

In summary, the performance monitoring program should have the following attributes:

- enough tests are included to provide meaningful data;
- the test is devised such that incipient degradation can reasonably be expected to be detected, and
- the licensee trends appropriate parameters as required by the ASME Code or ASME Code Case and as necessary to provide validation of the PRA.

DRAFT FOR COMMENT

Acceptance Guidelines

The acceptance guidelines for this item consists of evaluating the licensees proposed performance monitoring process to assure that it responds to the attributes listed in the preceding discussion. Assurance must be established that degradation is not significant for components that are placed on an extended test interval, and that failure rate assumptions for these components are not compromised by test data. It must be clearly established that sufficient testing is provided as part of the program to provide significant data, and that the test procedures and evaluation methods are implemented which provide reasonable assurance that degradation will be detected. Trending as appropriate should be performed by comparing parameters measured during RI- IST programs with the same parameters measured during the original IST programs.

5.3 Feedback and Corrective Action

If component failures or degradation occur at a higher rate than assumed in the basis for the RI- IST program, the following basic steps should be followed to implement corrective action:

- The cause(s) of the failures or degradation should be determined and corrective action implemented.
- The assumptions and failure rates used to categorize components according to risk should be reevaluated to determine if component importance rankings have changed.
- The equipment test effectiveness templates should be reevaluated, and the RI-IST program should be modified accordingly.

DRAFT FOR COMMENT

Acceptance Guidelines

- a. The licensee's corrective action program should evaluate RI-IST components that either fail to meet the test acceptance criteria or are otherwise determined to be in a nonconforming condition (e.g., a failure or degraded condition discovered during normal plant operation).
- b. The evaluation should:
 - (1) comply with 10 CFR 50, Appendix B, Criterion XVI, Corrective Action
 - (2) determine the impact of the failure or nonconforming condition on system/train operability since the previous test,
 - (3) determine and correct the root cause of the failure or nonconforming condition (e.g., improve testing practices, repair or replace the component),
 - (4) assess the applicability of the failure or nonconforming condition to other components in the RI-IST program (including any test sample expansion that may be required for grouped components such as relief valves),
 - (5) correct other susceptible RI-IST components as necessary,
 - (6) assess the validity of the PRA failure rate and unavailability assumptions in light of the failure(s), and
 - (7) consider the effectiveness of the component's test strategy in detecting the failure or nonconforming condition. Adjust the test interval and/or test methods, as appropriate, where the component (or group of components) experiences repeated failures or nonconforming conditions.
- c. The corrective action evaluations should be provided to the licensee's PRA group so that any necessary model changes and re-grouping are done as might be appropriate. The effect of the failures on plant risk should be evaluated as well as a confirmation that the corrective actions taken will restore the plant risk to an acceptable level.
- d. The RI-IST program documents should be revised to document any RI-IST program changes resulting from corrective actions taken.

DRAFT FOR COMMENT

5.4 Periodic Assessments

RI-IST programs should contain explicit provisions whereby component performance data periodically gets fed back into both the component categorization and component test strategy determination (i.e., test interval and methods) process.

Adequate program implementation requires that the RI-IST program results be predicted, monitored, and fed back into several key steps of the program development process.

Periodic assessments should be performed to reflect changes in plant configuration, component performance, test results, industry experience, and to reevaluate the effectiveness of the RI-IST program. These assessments should also take into consideration corrective actions that have been taken on past IST program components. Licensees should include in their RI-IST program proposals plans for these assessments, and they may wish to coordinate these reviews with other related activities such as periodic PRA updates, industry operating experience programs, the Maintenance Rule program, and other risk-informed program initiatives.

The assessment should:

- determine if component performance and conditions are acceptable (i.e., as compared to predicted or assumed levels). If performance and conditions are not acceptable then the cause(s) should be determined and corrective action implemented,
- review and revise as necessary the assumptions, reliability data, and failure rates used to categorize components to determine if component groupings have changed. Plant-specific data should be incorporated into the generic data using appropriate updating techniques, and
- reevaluate equipment performance as well as test effectiveness to determine if the RI-IST program should be adjusted (based on both plant-specific and generic information).

The licensee should have procedures in place to identify the need for more emergent RI-IST program updates (e.g., following a major plant modification, or significant equipment performance problem).

DRAFT FOR COMMENT

Acceptance Guidelines

The test strategy for RI-IST components should be periodically assessed (at least once every two refueling outages) to take into consideration results of RI-IST and new industry findings. The licensee's RI-IST program proposal should also include a plan for periodically assessing the plant PRA model to determine the need to incorporate new industry findings and new information resulting from the RI-IST program. (Plant specific data by itself cannot be the sole basis to determine component operability because the statistics will not be sufficient. Therefore, the RI-IST PRA model must also reflect industry experience.)

DRAFT FOR COMMENT

6. ELEMENT 4: DOCUMENTATION

The recommended format and content of an RI-IST submittal are presented in this chapter. Use of this format by licensees will help ensure the completeness of the information provided, will assist the NRC staff in locating the information, and will aid in shortening the time needed for the review process. Additional guidance on style, composition, and specifications of safety analysis reports is provided in the Introduction of Revision 3 to Regulatory Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)".

6.1 Risk-Informed Inservice Testing Program Plan

The licensee's submittal should describe the proposed RI-IST program with enough detail to be clearly understandable to the reviewers of the program. The description should cover the five items listed in Chapter 3 including sufficient detail such that reviewers of the program can understand how the program would be implemented in a phased approach. These items are: (1) changes to the plant's CLB, (2) changes to testing intervals and methods including a description of the process used for determining these, (3) listing of affected components including an explicit description of the grouping of different components in a staggered testing program, (4) identification of supporting information, and (5) brief statement regarding the way in which the proposed changes are consistent with the Commission's PRA Policy Statement. Also included should be a description of the process that was used for the categorization of components (further discussed in Section 6.2.3) and for the determination of when formal interaction with the NRC is or is not needed when making changes to an approved RI-IST program (Section 3.2). Exemptions from the regulations, technical specification amendments, and relief requests that are required to implement the licensee's proposed RI-IST program should also be given.

6.2 Probabilistic Risk Assessment Records and Supporting Data

6.2.1 Determination and Quantification of Accident Sequences

This section should present the methods and techniques used to identify and quantify any accident sequences that are specific to IST. Regulatory Guide DG-1061 includes more extensive guidance for this topic.

DRAFT FOR COMMENT

6.2.2 Initiating Events

The process used to identify initiating events and the results from the evaluation should be documented. The description of the process should include how it will result in the identification of the complete set of initiating events important to the supporting analysis, including those initiating events that may result from the failure of IST-affected components. For each initiating event identified by the process, present: (1) a description of the initiating event, (2) the rationale for including or excluding the event, (3) the event's frequency, and (4) a discussion of how frequency was estimated. If any individual initiating events are collapsed into a group, describe the basis for such a grouping. All information should be provided in the main report.

6.2.3 Categorization of Inservice Testing Components

In this section, the techniques used to categorize the RI-IST components should be discussed. When available, results from the categorization of the components from different viewpoints should be provided (e.g., traditional engineering analysis, probabilistic, and integrated). The technique used should be described including an identification of specific importance measures when used. The final results from the categorization should be presented in either one of two categories, high or low (i.e., HSSC or LSSC). The rationale used in the integrated decision-making process to place components in either category should be described for each component.

6.2.4 Assessment of Proposed Changes

This section should describe the estimated effect of the proposed RI-IST program changes on plant risk consistent with the general guidance given in Regulatory Guide DG-1061 and with the IST-specific guidance given in Section 4.2 of this regulatory guide.

6.2.5 Uncertainty/Sensitivity Analyses

The data used in any uncertainty calculations (i.e., uncertainty distributions for basic events or input parameters) and any sensitivity calculations (e.g., giving additional or less credit for operator actions than that considered in the base case) should be provided consistent with the guidance provided in Regulatory Guide DG-1061. How uncertainty was accounted for in the component categorization, and what sensitivity studies were performed to ensure the robustness of the categorization should be described.

DRAFT FOR COMMENT

6.2.6 Plant Data

Systems and Components Pertinent to IST

Summarize design and operating features of components and systems considered as part of the supporting analyses. Component records included with the submittal should clearly demonstrate the application of the specific criteria established by the licensee's integrated decision-making process (e.g., expert panel) to make a final determination of component grouping. Additional information that should be included in the proposal include specific ASME code cases that the licensee is implementing and the effected components. For each system, include a table summarizing key design and operating data. Such values used in the analysis should be identified and justified. Refer to appendices or other documents (e.g., specific sections of the USAR) as necessary for more details. Systems to be considered should include the pertinent portions of all systems credited in the plant-specific probabilistic analysis.

Plant Operating Experience

Summarize any events involving pump and valve failures that have occurred at this plant or similar plants. Include in this summary any lessons learned from these events and indicate actions taken to prevent or minimize recurrence of the events.

Operating Procedures

Present and describe the important operator actions as defined by existing procedures associated with events involving pump and valve failures. The descriptions should include what the operator is supposed to do and when it must be done. The conditions under which the operator takes each action, the expected time for performing the action, and how the time was derived should be identified. A summary of training materials associated with pump and valve failure events should be supplied. Include in this summary a synopsis of any simulator exercises associated with such events.

6.3 Integrated Decision Making Process Records

In addition to the general documentation requirements identified in Regulatory Guide DG-1061, provide a description of each issue considered in the integrated decision-making process and a discussion of how the resolution of each issue impacts the original probabilistic ranking. Information should be provided in the main report. Additional information specific to RI-IST programs regarding this important process is provided in the Appendix to this report.

6.4 Performance Monitoring Program

The licensee's program for monitoring the performance of both HSSC and LSSC components should be described. The licensee should have procedures developed to collect the following types of component performance data:

- Number of starts (or cycles) that each RI-IST component was subjected to under operational conditions and under test conditions,
- Number of failures that each RI-IST component experienced under operational conditions and under test conditions, and
- Number of hours that each RI-IST component was unavailable for corrective maintenance, preventive maintenance, and for testing.

6.5 Feedback and Corrective Action Program

As required by the current ASME Code, a record of each test should be maintained in which component failure occurred and corrective action was required. Procedures should be in place which are initiated by component failures that are detected by the RI-IST program as well as by other mechanisms (e.g., normal plant operation, inspections). Procedures should also exist to determine their impact on the plant PRA. Component-specific performance data should be used to support periodic PRA and RI-IST program updates.

6.6 Implementation Plans and Schedule

The licensee's implementation plans should be provided including a proposed schedule for initiating the program pending NRC approval. The phased implementation plan should state the composition of the component groupings for the staggered test strategy which are of the same type, size, manufacturer, model, and service conditions. Their staggered frequency over the test interval should also be included. Components should be identified that are to have their test intervals extended. The final test interval (at the maximum extended interval) of these components should also be included in the submittal.

DRAFT FOR COMMENT

7. REFERENCES

1. "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement," Federal Register, Vol. 60, p 42622, August 16, 1995.
2. U. S. Nuclear Regulatory Commission, "Framework for Applying Probabilistic Risk Analysis in Reactor Regulation," SECY-95-280, November 27, 1995.
3. U.S. Nuclear Regulatory Commission, "An Approach for Plant-Specific, Risk-Informed Decision Making: General Guidance," Regulatory Guide DG-1061 (draft)
4. U.S. Nuclear Regulatory Commission, "An Approach for Plant-Specific, Risk-Informed Decision Making: Inservice Inspection of Pipes," Regulatory Guide DG-1063 (draft)
5. U.S. Nuclear Regulatory Commission, "An Approach for Plant-Specific, Risk-Informed Decision Making: Graded Quality Assurance," Regulatory Guide DG-1064, (draft)
6. U.S. Nuclear Regulatory Commission, "An Approach for Plant-Specific, Risk-Informed Decision Making: Technical Specifications," Regulatory Guide DG-1065, (draft)
7. U.S. Nuclear Regulatory Commission, "Standard Review Plan for Risk-Informed Decision Making," Standard Review Plan, NUREG-0800, Chapter 19, (draft)
8. U.S. Nuclear Regulatory Commission, "Standard Review Plan for Risk-Informed Decision Making: Inservice Inspection of Pipes," Standard Review Plan, NUREG-0800, Chapter xx, (draft)
9. U.S. Nuclear Regulatory Commission, "Standard Review Plan for Risk-Informed Decision Making: Inservice Testing," Standard Review Plan, NUREG-0800, Sect. 3.9.7, (draft)
10. U.S. Nuclear Regulatory Commission, "Standard Review Plan for Risk-Informed Decision Making: Graded Quality Assurance," Standard Review Plan, NUREG-0800, Chapter xx, (draft)

DRAFT FOR COMMENT

11. U.S. Nuclear Regulatory Commission, "Standard Review Plan for Risk-Informed Decision Making: Technical Specifications," Standard Review Plan, NUREG-0800, Chapter xx, (draft)
12. ASME research document, "Risk-Based In-Service Testing - Development of Guidelines, Volume 2, Light Water Reactor (LWR) Nuclear Power Plant Components," 1995
13. "ASME Code Case for IST Component Importance Ranking," (draft January 1997)
14. EPRI TR-105396, "PSA Applications Guide," August 1995
15. "Nuclear Energy Institute Industry Guideline for Risk-Based Inservice Testing," (NEI draft Rev A), September 20, 1995.
16. Nuclear Energy Institute Draft (Revision B) "Industry Guidelines for Risk-Based Inservice Testing" dated March 19, 1996.
17. ASME Supporting White Paper, "ASME Code Case for IST Component Importance Ranking," (draft January 1997)
18. U. S. Nuclear Regulatory Commission, NUREG-1602, "A Standard for Probabilistic Risk Assessment (PRA) to Support Risk- Informed Decisionmaking, (draft)
19. U. S. Nuclear Regulatory Commission, (regulatory guide for proposed data rule), Regulatory Guide DG-1046 (draft)
20. Common Cause Failure Data Collection and Analysis System, Volumes 1-6, INEL-94/0064, December 1995

DRAFT FOR COMMENT

APPENDIX A. DETAILED GUIDANCE FOR INTEGRATED DECISION MAKING

A.1 Introduction

The increased use of probabilistic risk assessment (PRA) in nuclear plant activities such as in risk-informed inservice testing (IST) programs will require a balanced use of the probabilistic information with the more traditional engineering (sometimes referred to as "deterministic") information. Some structured process for considering both types of information and making decisions will be needed that will allow improvements to be made in plant effectiveness while maintaining adequate safety levels in the plant. This will be particularly important during initial program implementation and also for the subsequent early phases of the program. In some instances, the physical data from the PRA and from the deterministic evaluations may be insufficient to make a clearcut decision. At times, these two forms of information may even seem to conflict. In such cases, it is the responsibility of the licensee to assemble the appropriate skilled utility staff (and in some cases consultants) to consider all of the available information in its various forms and to supplement this information with engineering judgment to determine the best course of action. The participants involved in this important role have generally been referred to in various industry documents¹⁴⁻¹⁹ as an "Expert Panel." In this appendix, this functional activity will be described as being an engineering evaluation without specifying how the evaluation is to be performed administratively. It is not the intention of this guidance to indicate that a special administrative body needs to be formed within the utility to satisfy this role. It is the function that is important and that must be performed in some well-organized, repeatable, and scrutable manner by the licensee. This functional activity is all pervasive in the implementation phase of such activities as inservice inspection (ISI) and IST, and accordingly, the responsibility of the licensee to see that this function is done well is great.

A.2 Basic Categories of Information To Be Considered

Risk importance measures may be used together with other available information to determine the relative risk ranking (and thus categorization) of the components included in the evaluation. Results from all of these sources are then reviewed prior to making final decisions about where to focus IST resources.

Although the risk-ranking of components can primarily be used as the basis for prioritizing IST at a plant, additional considerations need to be addressed (e.g., defense in depth, common cause, and the single failure criterion) which may be more constraining than the risk-based criteria in some cases. Consideration must be given to these issues before the IST requirements for the various

DRAFT FOR COMMENT

components are determined.

IST experience should contribute an understanding of the important technical bases underlying the existing testing program before it is changed. The critical safety aspects of these bases should not be violated inadvertently in changing over to a RI-IST, and important plant experience gained through the traditional IST should be considered during the change.

The plant-specific PRA information should include important perspectives with respect to the limitations of PRA modeling and analysis of systems, some of which may not be explicitly addressed within the PRA analysis. An understanding should also be provided as to how the proposed changes in pump and valve testing could affect PRA estimates of plant risk.

Plant safety experience should provide insights associated with the traditional analyses (Chapter 15 of the plant Final Safety Analysis Report) and any effect that proposed changes in testing might have on the traditional perspective of overall plant safety.

Plant operational input should supplement the insights of plant safety with additional information regarding the operational importance of components under normal, abnormal, and emergency conditions. There should also be input on operating history, system interfaces, and industry operating experience to supplement information from the IST.

Maintenance considerations should provide perspectives on work practices, implementation of the maintenance rule, and equipment operating history.

Systems design considerations should include the potential effect of different design configurations (e.g., piping, valves, and pumps) on planning for a risk-informed IST, particularly if future plant modifications are contemplated or if systems are temporarily taken out of service for maintenance or replacement or repair.

A.3 Specific Areas To Be Evaluated

This section addresses some technical and administrative issues that are currently believed to be particularly important for IST risk-informed applications. Additional issues of a more general nature that may arise in expert panel deliberations are given in the general SRP and in Regulatory Guide DG-1061.

DRAFT FOR COMMENT

- Each safe-shutdown function, such as reactivity control, reactor coolant system integrity, coolant inventory control, primary system heat removal, etc. (or use the Appendix R safe-shutdown function paths), should retain one system that is considered more safety significant with pump and valve testing planned accordingly. In other words, a minimum set of high safety significant equipment should be operable to maintain defense-in-depth.
- It should be confirmed that pump and valve classifications have given proper attention to systems identified in emergency operating procedures (and other systems) depended upon for operator recovery actions, primary fission product barriers excluded from the PRA due to their inherent reliability (such as the RPV), passive items not modeled in the PRA (such as piping, cable, supports, building or compartment structures such as the spent fuel pool), and systems relied upon to mitigate the effects of external events in cases where the PRA considered only internal events.
- Failure modes modeled by the PRA may not be all-inclusive. Consideration should be given to the failure modes modeled and the potential for the introduction of new failure modes related to the IST application. For example, if valve mispositioning has been assumed to be a low-probability event because of independent verification and therefore is not included in the PRA assumptions, any changes to such independent verifications should be evaluated for potential impact on the PRA results. Reverse flow in check valves should be evaluated.
- Other qualitative/quantitative analyses that shed light on the relative safety importance of components, such as FMEA, shutdown risk, seismic risk, SBO/ATWS/fire protection should be included in the resource information base.
- Attention should be given to the fact that component performance can be degraded from the effects of aging and this issue will need to be addressed and documented.
- The engineering evaluation should include the choice of new test frequencies, the identification of compensatory measures for potentially important components, and the choice of test strategies for the HSSCs.
- Until the ASME recommendations for improved test methods are available, the different existing IST test methods should be evaluated prior to choosing the test methods to be used for the HSSCs depending on their expected failure modes, service conditions, etc.
- Due to the importance of maintaining defense in depth, particular attention should be given to identifying any containment systems involving IST components.



U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

March 1997
Draft DG-1064

DRAFT REGULATORY GUIDE

Contact: H. W. (Roy) Woods (301)415-6622

An Approach for Plant-Specific, Risk-Informed Decision Making: Graded Quality Assurance

Draft for Comment

MARCH 24, 1997

This regulatory guide is being issued in draft form to involve the public in the early stages of the development of a regulatory position in this area. It has not received complete staff review and does not represent an official NRC staff position.

Public comments are being solicited on the draft guide (including any implementation schedule) and its associated regulatory analysis or value/impact statement. Comments should be accompanied by appropriate supporting data. Written comments may be submitted to the Rules Review and Directives Branch, DFIPS, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555. Copies of comments received may be examined at the NRC Public Document Room, 2120 L Street NW., Washington, DC. Comments will be most helpful if received by

Requests for single copies of draft or active regulatory guides (which may be reproduced) or for placement on an automatic distribution list for single copies of future draft guides in specific divisions should be made in writing to the U.S. Nuclear Regulatory Commission, Washington, DC 20555, Attention: Distribution and Mail Services Section, or by fax to (301)415-2260.

TABLE OF CONTENTS

| Chapter | | Page |
|--|---|------|
| 1. INTRODUCTION | | 1-1 |
| 1.1 | Background | 1-1 |
| 1.2 | Purpose and Scope | 1-3 |
| 1.3 | Organization and Content | 1-3 |
| 1.4 | Relationship to Other Guidance Document Applications | 1-4 |
| 2. PROCESS OVERVIEW | | 2-1 |
| 3. ELEMENT 1: DEFINE THE PROPOSED CHANGES | | 3-1 |
| 4. ELEMENT 2: ENGINEERING EVALUATION | | 4-1 |
| 4.1 | Safety Significance Categorization | 4-1 |
| 4.1.1 | Identification of System Functions | 4-2 |
| 4.1.2 | System Function Safety Significance Categorization | 4-2 |
| 4.1.2.1 | Quantitative Safety Categorization Insights | 4-3 |
| 4.1.2.2 | Qualitative Safety Categorization Insights | 4-4 |
| 4.1.3 | Identification of Components Which Support Functions | 4-5 |
| 4.1.4 | Component Safety Significance Categorization | 4-7 |
| 4.2 | Demonstration of Conformance with Safety Principles | 4-8 |
| 4.3 | Integrated Assessment | 4-10 |
| 5. ELEMENT 3: DEVELOP IMPLEMENTATION AND MONITORING STRATEGIES | | 5-1 |
| 5.1 | Grading of Quality Activities | 5-1 |
| 5.1.1 | Regulations | 5-1 |
| 5.1.2 | Grading of Quality Elements | 5-2 |
| 5.2 | Potential Areas for Implementing Graded QA Program Controls | 5-3 |
| 5.2.1 | Procurement | 5-4 |
| 5.2.2 | Frequency of Inspections | 5-4 |
| 5.2.3 | Records and Documentation | 5-4 |
| 5.2.4 | Audits | 5-5 |
| 5.2.5 | Staff Training and Qualification Requirements | 5-5 |
| 5.2.6 | Corrective Action | 5-5 |
| 5.3 | Performance Monitoring | 5-5 |
| 5.3.1 | Operational Feedback | 5-6 |
| 5.3.2 | Corrective Actions | 5-7 |
| 6. ELEMENT 4: DOCUMENTATION | | 6-1 |
| 6.1 | GQA Program | 6-1 |
| 6.2 | Plant Data | 6-2 |
| 6.2.1 | Systems Pertinent to GQA | 6-2 |
| 6.2.2 | Status of SSCs | 6-2 |
| 6.2.3 | Plant Operating Experience | 6-2 |
| 6.2.4 | Engineering Evaluation | 6-2 |
| 7. REFERENCES | | 7-1 |

LIST OF FIGURES

| Figure | Page |
|--|------|
| Figure 2.1 General description of an acceptable approach to risk-informed applications | 2-3 |

1. INTRODUCTION

1.1 Background

The NRC has promulgated deterministic criteria for determining which commercial nuclear power plant equipment is considered safety-related (see 10 CFR 50.2, Appendix A to 10 CFR 100, 10 CFR 50.65, and 10 CFR 50.49). Because of the importance of the safety-related equipment to protect public health and safety, the NRC has additionally required that a Quality Assurance (QA) program (described in Appendix B to 10 CFR 50) be applied to all activities affecting the safety-related functions of that equipment. The overall purpose of the QA program is to establish a set of systematic and planned actions that are necessary to provide adequate confidence that safety-related plant equipment will perform satisfactorily in service. The requirements delineated in Appendix B to 10 CFR 50 recognize that QA program controls should be applied in a manner consistent with the importance to safety of the associated plant equipment. In the past, engineering judgement provided the general mechanism to determine the relative importance to safety of plant equipment.

In recognition of advances made in the state-of-the-art in the Probabilistic Risk Assessment (PRA) technology area, the NRC has made the decision to expand the use of PRA in the regulatory process. PRA will provide new insights that may be utilized by licensees to determine the relative safety-significance of plant equipment. The probabilistic insights could then be utilized to help identify low safety significant Structures, Systems, and Components (SSCs) that are candidates for reductions in QA treatment. The end result of this process could be that licensees would have plant equipment that is typically categorized as follows: safety-related and high-safety-significant; safety-related and low-safety-significant; non-safety-related and high-safety-significant; and non-safety-related and low-safety-significant. Grading of QA controls would vary commensurate with these categorizations. This document provides guidance that could be used by licensees to determine both the relative safety significance of plant equipment, and to adjust the application of QA controls accordingly.

Requirements related to quality assurance (QA) programs for nuclear power plants are set forth in Appendix B to Part 50 of Title 10 of the Code of Federal Regulations (10 CFR 50). The general statements contained in Appendix B are supplemented by industry standards and NRC regulatory guides which describe specific practices that have been found acceptable by the industry and NRC staff. Although both Appendix B and the associated industry standards allow a large degree of flexibility, the licensees and the Nuclear Regulatory Commission (NRC) staff have been reluctant to make major changes in established QA practices. Recently, however, changes in the nuclear industry have resulted in numerous proposals to revise QA practices. These changes include the completion of construction projects, establishment of programs related to plant operations and maintenance, maturing of licensee programs and personnel, and increased pressures to control plant operating costs.

Graded Quality Assurance (GQA) is intended to provide a safety benefit by allowing licensees and NRC to preferentially allocate resources based on the safety significance of the item. The Commission has articulated its expectation that implementation of the policy to expand the use of Probabilistic Risk Assessment (PRA) will improve the regulatory process in three areas: foremost through safety decision

Draft for Comment

Introduction

making enhanced by the use of PRA insights; through more efficient use of agency resources; and through a reduction in unnecessary burdens on licensees. Background information about initial efforts to implement GQA is given in SECY-95-059, "Development of Graded Quality Assurance Methodology" (March 10, 1995).

Licensees developing GQA programs will adjust their QA programs to accommodate their individual needs. The NRC conveyed its goals and expectations for an acceptable graded QA program to Nuclear Energy Institute (NEI) on June 15, 1994. Irrespective of a licensee's specific approach, the NRC stated a graded QA program should have four essential elements:

- (1) a process that determines the safety significance of structures, systems, and components (SSCs) in a reasonable and consistent manner including the use of both traditional engineering and probabilistic evaluations
- (2) the implementation of appropriate QA controls for SSCs, or groups of SSCs, according to safety function and safety significance to maintain reasonable confidence in equipment performance and to support the GQA corrective action feedback process
- (3) an effective root-cause analysis and corrective action program
- (4) a means for reassessing SSC safety significance and QA controls when new information becomes available through operating experience, or based on changes in plant design

Also, during the last several years, both the NRC and the nuclear industry have recognized that probabilistic risk assessment (PRA) has evolved to the point where it may be used as a tool in regulatory decision making so that the regulations can be implemented more effectively. In 1995, the NRC issued a final policy statement on the use of PRA methods in nuclear regulatory activities. In its approval of the policy statement, the Commission articulated its expectation that:

- The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.
- PRA and associated analyses (e.g., bounding analyses, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices. Where appropriate, PRA should be used to support the proposal of additional regulatory requirements in accordance with 10 CFR 50.109 (backfit rule). Appropriate procedures for including PRA in the process for changing regulatory requirements should be developed and followed. It is, of course, understood that the intent of this policy is that existing rules and regulations shall be complied with unless these rules and regulations are revised.

- PRA evaluations in support of regulatory decisions should be as realistic as practicable, and appropriate supporting data should be publicly available for review.
- The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgments on the need for proposing and backfitting new generic requirements on nuclear power plant licensees.

The staff's review of 10 CFR Part 50 indicates that the option of applying QA measures in a manner commensurate with safety significance is clearly available to licensees. That is, no exemptions from current regulations are expected to be needed to implement a Graded Quality Assurance (GQA) program. The implementing industry QA standards (which licensees have committed to implement to fulfill the requirements of Appendix B) also contain general provisions for applying QA using a graded approach. However, when implementing such changes, licensees may need to submit a revised QA program to the staff pursuant to 10 CFR 50.54(a).

1.2 Purpose and Scope

In this guide the staff describes an acceptable approach for identifying the safety significance of SSCs and assigning QA controls accordingly to ensure that QA requirements are being graded commensurate with safety. This regulatory guide contains guidance that allow licensees to modify their current QA program controls based on the safety categorization of the SSCs. This regulatory guide also describes an acceptable approach for monitoring the effectiveness of the GQA program implementation, and for determining when it may be necessary to make adjustments in quality assurance practices and safety significance categorizations to ensure that SSCs remain capable of performing their intended functions. The guide also delineates the principles for risk-informed decision making, or guiding features, of a GQA program that need to be dealt with by a licensee. In some cases rather than articulating a prescriptive method that must be implemented by a licensee to fulfill these principles (or their subsidiary issues) for GQA, the staff has chosen to identify those issues which must be evaluated, and documented, by a licensee when formulating their particular approach to GQA. Thus, the burden would fall on the licensee to be able to inform the staff how the issues were addressed within their site specific program.

1.3 Organization and Content

Limited data is available to define the impact of quality assurance programs on SSC performance. Consequently, this regulatory guide emphasizes the classification of equipment into two or more safety significance categories as discussed in "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis " (Reference 25). Chapter 2 provides an overview of the four-element process used for implementing risk-informed GQA. Chapter 3 provides a discussion of Element 1, a definition of proposed changes to QA applications; Chapter 4 discusses element 2 and addresses engineering evaluations applicable to GQA programs; Chapter 5 discusses element 3 and provides specific guidance for an acceptable approach for implementing graded quality assurance controls and for developing performance monitoring strategies ; The documentation and submittal aspects related to the change (element 4) is specified in Chapter 6.

1.4 Relationship to Other Guidance Document Applications

"An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis " (Reference 25) describes a general approach to risk-informed, regulatory decision making and includes a discussion of specific topics common to all regulatory applications. This regulatory guide provides guidance specifically for GQA programs, consistent with but more detailed than the generally applicable guidance given in the "overall" guide (Reference 25).

Licensees may choose to use risk-informed decision making in application areas other than Graded QA. It is anticipated that certain efficiencies could be realized in that situation. It is possible that a single list of SSCs could be defined as safety significant for multiple risk-informed applications if a sufficiently robust process were utilized.

2. PROCESS OVERVIEW

As the nuclear industry incorporates risk insights into its QA programs, it is anticipated that the industry will build upon its existing risk-informed activities, including the individual plant examination program. To provide the industry with the NRC's expectations for risk-informed decision making, a regulatory guidance document, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis " (Reference 25), was developed which establishes five safety principles, and describes a 4-element process for evaluating risk-informed regulatory changes consistent with addressing those principles, as illustrated in Figure 2.1. Reference 25 provides additional description of quantitative acceptance guidelines, discussion on defense-in-depth aspects, and addresses safety margins. The principles are:

1. The proposed change meets the current regulations. This principle applies unless the proposed change is explicitly related to a requested exemption or rule change.
2. Defense-in-depth is maintained.
3. Sufficient safety margins are maintained.
4. Proposed increases in risk, and their cumulative effect are small and do not cause the NRC Safety Goals to be exceeded.
5. Performance-based implementation and monitoring strategies are proposed that address uncertainties in analysis models and data and provide for timely feedback and corrective action.

The individual elements of this process are described in the general guidance document. Those generally applicable discussions are not repeated here. Instead, an acceptable method and issues to be addressed by the licensee to fulfill the guiding principles, is described for categorizing SSCs at nuclear power plants in a manner commensurate with their safety significance (using integrated traditional engineering, qualitative, and probabilistic insights), and for applying appropriate QA programs to each category of SSCs.

The process described below begins with a set of actions related to proposed changes in the QA categorization of certain SSCs. The process for developing the initial proposal for the changes is left to the utility, but it should derive from an examination of both traditional engineering and probabilistic information, and it should result in categorization of the plant's SSCs based on their safety significance so that an appropriate level of quality controls can be applied (see further discussion under "Element 1" below).

Element 1: Define the Proposed QA Program Change

In this element, the licensee identifies the scope of candidate SSCs, and associated activities, for a risk-informed application of QA requirements including:

- a) systems and components that are subject to current Appendix B QA requirements,

Process Overview

- b) SSCs modeled in the PRA for the plant,
- c) non-safety related SSCs that are within the Maintenance Rule scope, and
- d) non-safety related equipment that has previously received augmented quality treatment (e.g., Anticipated Transient Without Scram, Station Blackout, Fire Protection).

The licensee should ensure that the QA program commitments and other QA related information on the docket, germane to the contemplated changes in QA practices, are clearly understood and adhered to, unless modified or amended through the appropriate licensing or regulatory actions. The suitability of the plant-specific PRA should be assessed relative to its use in supporting the GQA decision-making process. And, available industry and plant-specific operational experience information relative to GQA should be assessed.

Further, the licensee should also identify the overall objective and approach of the proposed changes to the QA program for the candidate SSCs. More details are provided in Chapter 3 of this document.

Element 2: Engineering Evaluations

In element 2, the proposed changes in the application of QA controls for SSCs as a function of categorization commensurate with safety are examined and assessed with respect to the relevant risk-informed decision making safety principles. An essential element of the evaluation is the categorization of SSCs into high and low safety significant categories. The impact of the QA program changes on defense-in-depth would be determined through the use of both traditional engineering evaluations and probabilistic risk assessment techniques. In addition, an assessment is required to ensure that no more than small risk increases are introduced by the proposed changes, as described in Chapter 4. The engineering evaluation helps to establish the safety significance of systems and components and determines that the effects of the changes in QA controls has a small impact on plant risk. More details concerning element 2 are contained in Chapter 4.

Element 3: Develop Implementation and Performance Monitoring Strategies

The third element involves developing graded QA control implementation and monitoring plans. These plans should be formulated to assure that appropriate system and component performance are maintained. For the safety-related SSCs in the high safety significant category, no changes in QA controls are expected to be proposed. For the non-safety-related SSCs which are found to be safety-significant, an evaluation would be performed to determine what augmentation of existing QA controls is appropriate. For low safety significant SSCs that are safety-related, reductions in QA controls are anticipated. Means should be specified for monitoring the performance of systems and components and of quality related activities and processes, and for applying corrective actions. Specific guidance for element 3 is provided in Chapter 5.

Element 4: Document Evaluations and Submit Request

The final element involves documenting the analyses for staff or independent review, audit or inspection, and submitting the request to change implementation of QA commitments, as required by 10 CFR 50.54(a) if the change involves a reduction in the licensee's QA commitments. If the proposed change does not involve a reduction in the licensee's QA commitments, then prior staff review and approval is not required and the change to the QA program is submitted in accordance with 50.71(e). The changes associated with the adoption of graded QA proposed by the licensee will be described in the QA Program. In addition, important assumptions including SSC functional capabilities, impact of failure on safety significant functions, and performance attributes, which play a key role in supporting the acceptability of the QA program change, should be identified by the licensee in the QA program.

Documentation necessary to support the graded QA effort is listed in Chapter 6 of this regulatory guide.

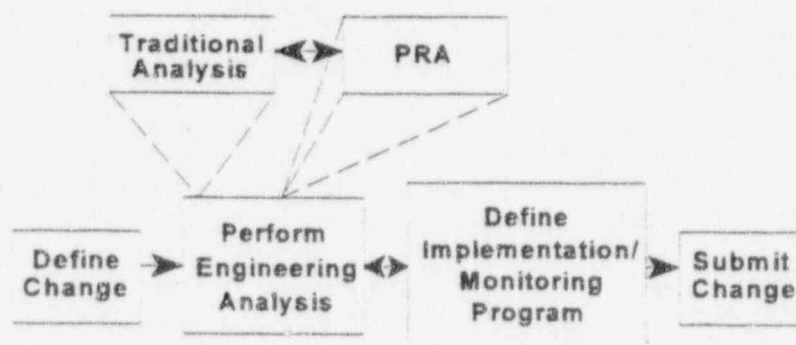
INTEGRATED DECISION

Figure 2.1 General description of an acceptable approach to risk-informed applications.

3. ELEMENT 1: DEFINE THE PROPOSED CHANGES

The first element in the process of evaluating a change to GQA programs involves providing a full definition of the change. The first step is to identify the overall scope of the QA program in terms of the SSCs that are covered. Additionally, the licensee's PRA would be evaluated with respect to its adequacy to support the GQA decision making process. To accomplish this the licensee should:

1. Identify the set of regulatory requirements and commitments that are directly related to the proposed QA implementation changes as well as those that may be impacted. This information is used to demonstrate that the proposed QA changes do not violate existing regulatory requirements. The major regulatory requirements applicable to GQA programs are set forth in 10 CFR 50, Appendices A and B, 10 CFR 50.54(a), and 10 CFR 50.34. Changes to technical requirements are controlled under existing processes such as 10 CFR 50.59, license amendments, relief requests, and exemption requests, which are outside of the scope of this document. Relevant quality commitments that are to be considered reside in a variety of licensing documentation such as the QA program description, the final safety analysis report, responses to generic communications, and responses to enforcement actions.
2. Identify the structures, systems, and components (SSCs) and associated activities that are candidates for assessment within the risk-informed application of graded QA requirements. Candidate SSCs include those that are (a) subject to current Appendix B QA requirements, (b) SSCs modeled in the licensee's PRA for the plant, and (c) non-safety related SSCs that are within the Maintenance Rule scope (which includes the non-safety related SSCs I) relied upon to mitigate accidents; ii) that are used in emergency operating procedures; iii) those whose failure could prevent a safety-related SSC from performing its safety-related function; and iv) those whose failure could cause a reactor scram or actuation of a safety-related system). In addition, non-safety related equipment that has previously received augmented quality treatment (e.g., Anticipated Transient Without Scram, Station Blackout, Fire Protection) should be considered in the GQA application scope.
3. Identify the expected revisions to existing implementing guidance of QA requirements that will result from the graded QA program. No exemptions from current regulations are expected to be needed to implement a GQA program. However, the commitments of each licensee regarding QA are addressed in a number of documents including the Final Safety Analysis Report (FSAR), a QA topical report (if applicable), and other docketed correspondence (e.g., responses to generic communications, inspection reports, etc). Licensees are expected to maintain control of their licensing bases. Accordingly, changes in QA program commitments should be identified and the manner in which they are being changed should be documented, reviewed, and approved by the NRC in accordance with 10 CFR 50.54(a).
4. The licensee should evaluate its risk studies to determine the extent to which quantitative and qualitative risk insights may be utilized. The quality, level of review of, and accuracy of plant representation of the risk studies should also be taken into account when determining the level of support the studies can provide to the development and implementation of the graded QA

Draft for Comment

Define The Proposed Changes

program. The licensee should also consider how it may use risk study models, computer programs, and personnel to support the long term performance monitoring program required as part of graded QA implementation.

5. The licensee should not make any changes in the application of QA controls and processes prior to the evaluation of the associated system or component to determine its safety significance as discussed in Chapter 4 and receive subsequent approval of the QA changes by the NRC if required.

The definition of the change should be completed by categorizing the SSCs identified above according to whether they are high- or low-safety-significant. For those safety-related SSCs that are categorized as high-safety-significant, current QA practices would apply. For those non-safety-related SSCs that are high safety significant, some increase in QA controls may be warranted and should be implemented where appropriate. For those safety-related SSCs that are low-safety-significant, relaxation in QA controls may be proposed. For non-safety-related SSCs that are low-safety-significant, licensees would continue to define their quality controls.

4. ELEMENT 2: ENGINEERING EVALUATION

In Regulatory Guide DG-1061, "An Approach for Using Probabilistic Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis " (Reference 25), Element 2 is the engineering evaluation conducted to support decisions to change a plant's licensing bases. Changes in the application of QA controls do not lend themselves to a quantitative assessment because the relationship between QA programs and equipment performance (and, hence, risk contribution) has not been explicitly established. Furthermore, only a small fraction of components that are candidates for application of graded QA controls are explicitly modeled in PRAs. This small percentage arises from PRA's emphasis on the control and mitigation of severe accidents and exclusion of equipment such as recombiners useful only for control of design basis accidents, the exclusion of most instrumentation and reactor protection system equipment from the models, the exclusion of emergency preparedness and monitoring equipment from the models, combining of SSCs with identical failure consequences into grouped basic events, and not including some highly reliable SSCs when other less reliable SSCs (of similar impact) or operator actions are modeled.

Categorization of the safety significance of components for utilization in Graded QA should be accomplished through the use of traditional engineering evaluations in combination with quantitative risk importance measures and qualitative risk insights. Such a combined, "integrated" approach is necessary to utilize the strengths and avoid inherent limitations in each method. Regulatory Guide DG-1061 discusses applications where risk insights are characterized by calculated risk importance measures or bounding estimates, or a qualitative assessment where the anticipated risk impact is minimal.

4.1 Safety Significance Categorization

A minimum of two levels of categorization are needed, preferably labeled high- and low-safety-significant. At the prerogative of the licensee, a greater number of safety significance levels can be defined, such as three levels comprised of high/medium/low safety significance. From a regulatory point of view, it is essential to assure that high-safety-significant items are not inappropriately categorized as less-than-high since these might then be inappropriate candidates for reduced QA requirements. Therefore, for regulatory purposes, high safety significance may be assumed or assigned. Only assignments of low (medium, etc.) safety significance must be justified.

Systems have a variety of operating modes and perform a variety of functions, where each function is a well defined task requiring the proper operation of some sub-set of system equipment. Although certain QA controls are applied at the component or even piece part level, safety significance categorization is most appropriately defined at the system function level. Therefore, the guidance in this document is based on determining the safety significance of system functions, identifying the components and component operational modes required to support high-safety-significant functions, and determining the categorization of the components based on this information. The linkage between the functions a system performs and the components required to support each function is most clearly established in a matrix format as described in Section 4.1.3.

The categorization process must also systematically identify and track system functional boundaries, defined as the point (component) at which a system operating in a particular mode functionally interfaces with a connected system. The categorization of the safety significance of support functions is generally determined by the categorization of the function being supported, augmented by a quantitative or qualitative evaluation of the support system's aggregate safety significance. Interfacing function categorization should be well documented, traceable, and internally consistent.

The quality, scope, and level of detail of the PRA should be commensurate with the extent that the PRA is used in the categorization process. As discussed in Regulatory Guide DG-1061, the baseline risk profile and the magnitude of the anticipated change in risk are important considerations in the determination of the acceptability of risk informed applications. The licensee must demonstrate that the PRA is of sufficient quality to support a decision on the acceptability of the proposed change.

All operational modes and internal and external events should be included in the evaluation of the safety significance of systems, functions, and components. At a minimum, models and results for core damage and large early release frequency for internal initiating events at full power are needed. If quantitative risk analyses for shutdown conditions and "external" initiators such as fire, seismic, and winds are not available, qualitative assessments should be used to ensure the functions' safety significance categorization fully considers all relevant operational demands. Qualitative studies identify and characterize scenarios that are believed to be important, but without expending significant resources in quantifying the scenarios' frequencies. Seismic margin analysis and FIVE evaluations done to support IPEEE analyses are examples of qualitative studies which should be used.

4.1.1 Identification of System Functions

Definition of the proposed change includes the identification of all the functions a system must perform. Although many system functions may eventually be categorized as low-safety-significant, characterization of the proposed change begins with a description of all functions a system must fulfill. System functions should include functions used during normal operation as well as all functions related to the prevention or mitigation of core damage, protection of containment integrity, or reduction in the release probability or consequence to the public from accidents and transients both within and beyond the design basis (e.g., risk analysis).

4.1.2 System Function Safety Significance Categorization

Determination of the safety significance of system functions is inherently a "top down" process starting with the front line systems and system functions directly involved in plant level safety functions (such as reactivity control, reactor pressure control, and decay heat removal). The delivery of high pressure primary coolant from the reactor water storage tank to the core may be categorized as a high-safety-significant function. The pumps, valves, and other SSCs whose proper operation is required to fulfill this function derive their categorization from the significance of the function. Therefore, any determination of an SSC's safety significance requires determination of the safety significance of all functions the SSC supports. Similarly, determination of the safety significance of support system

functions (which should be later pursued in the support system's evaluation) is best performed by determining the safety significance of the function being supported.

Licensees may limit their evaluation to the system level and conservatively judge all components in a high-safety-significant system to be high-safety-significant, or they may further categorize components within systems based on the safety significance of the functions each component supports. To provide confidence that eventual determination of less than high-safety-significance is made with full recognition of each system's contribution to CDF and LERF, system-level importance should be determined even when function- or component-level importance measures are available.

PRA's integrated models provide an excellent framework to characterize system and system function importance. One area where PRA modeling is not fully adequate for graded QA applications is, however, cross-system dependencies arising from nominally identical components used in different applications throughout the plant (a type of circuit breaker, for example). Cross-system dependencies are not modeled in PRAs yet can have a significant impact on risk. Consequently, special consideration must be given to these sets of components as discussed in 4.2.

4.1.2.1 Quantitative Safety Categorization Insights

Quantitative importance measures from risk studies provide valuable insights about the relative ranking of the safety significance of well defined model elements in the PRA model such as basic events, components, human actions, functions, trains, or systems. Each measure represents the risk sensitivity of an individual model element. Once one element is varied, the importance measures for the other elements will change. Consequently, while large or small importance measure values identify candidate high- or low- safety-significant model elements, final categorization is determined during the integrated decision making.

At least two quantitative measures of importance are needed, one (such as Fussell-Vesely (FV) or risk reduction worth (RRW)) illustrating the fraction of current risk involving the failure of the model element, the other (such as risk achievement worth (RAW) or Birnbaum) illustrating the margin of safety contributed by the model element's proper operation. Other measures than those suggested may be used, but at least two measures reflecting current contribution and margin contribution are needed to balance the risk insights. A number of issues associated with the calculation and interpretation of importance measures are discussed in Appendix A of DG-1061. The licensee needs to be able to describe technically how each issue discussed in Appendix A was addressed and resolved.

System and system function level measures are difficult to define and calculate and alternative techniques for categorizing the safety significance of functions may be more practical. One alternative technique uses basic event importance measures (readily calculated by most PRA codes) to identify a set of system functions which are clearly high-safety-significance. This technique is based on recognition that the system and system function RAW and FV importance measures will always be at least as large as the RAW and FV for basic events whose failure will fail the function (if other importance measures and this technique are used, this property should be validated for the measures used).

The basic event importance measures¹ should be calculated and compared to some quantitative guideline values (e.g., $RAW > 2$ or $FV > 0.005$; the specific values chosen should be justified by the licensee). All basic events with importance measure greater than (or less than, as appropriate) the guidelines are identified as potentially high-safety-significance basic events. Any system function modeled in the PRA which is supported by one or more potentially high-safety-significant basic events is categorized as a candidate high-safety-significant system function. Since it is possible that the system's and system function's RAW and FV measures are much higher than any individual basic event's, systems and system functions not categorized as candidate high should, as a minimum, be further evaluated as discussed below, and the licensee should describe technically how each issue was addressed

- The redundancy and reliability of trains within systems that are available to fulfill a critically important system function can have the result that each individual basic event within the system has very low importance measure values or is even truncated out of the results. A system function-based analysis should be performed to determine the impact of the failure of candidate low-safety-significant systems. Discrepancies in the form of high failure consequence for some systems (automatic depressurization system, for example) but low or no basic event importance measures should be identified and the relevant high-safety-significant functions defined.
- Initiating events are usually not modeled as basic events or, if they are, are modeled as single modularized events. Some examples of such initiating events are the loss of instrument air, the loss of main feedwater, the loss of offsite power (through local switchyard faults), the loss of alternating current (AC) or direct current (DC) buses. If components whose failure contributes to these initiating events are modeled in other initiating events (i.e., loss of an air compressor leading to loss of pneumatic valves following a loss of component cooling), the importance of the basic events will not include the contribution of the failure to the initiating event frequency. Thus, the importance of functions whose failure would both cause an initiating event as well as the partial loss of mitigating function can be severely underestimated by surrogate basic event importance measures.

4.1.2.2 Qualitative Safety Categorization Insights

PRA results are to be used in conjunction with traditional engineering, and the principles associated with defense in depth and safety margins must also be factored into the safety significance determination. Consequently, the following qualitative factors should be applied to the quantitative PRA insights developed in the previous section. The licensee needs to be able to describe technically how each issue was evaluated and resolved.

- The diversity of systems that are able to fulfill critical high level functions (i.e., reactivity control, decay heat removal, etc.) can have the result that each individual system could meet all quantitative guidelines to be categorized in the low safety significance group. It would be prudent, and the licensee is expected, to designate at least one system associated with critical high level functions as high-safety-significant.

- Screening analyses are used to dismiss some functional failures as insignificant. In many cases, credit for the redundancy or reliability of plant systems or structures is taken to bolster the arguments that the functional failure need not be modeled. Thus, the importance of some systems, functions, and structures will not show up in the PRA results since the functional failure is screened out. (For example, screening out of certain containment penetrations because of the number of isolation valves involved obscures the importance of the containment isolation function of the system)
- Risk insights from non-quantitative risk studies should also be used. Transients initiated during shutdown or initiated by external events such as earthquakes, high winds, and fires are often evaluated without developing and quantifying full probabilistic models. Nevertheless, these studies include information on the systems, functions, and components whose proper operation is credited in the defense against such transients. In particular, it is shown how the plant is intended to respond to such events, and, further, what alternative strategies are available if the preferred strategy fails. When such studies are not included in the quantitative safety significance categorization, all the systems and functions credited in these studies should be categorized as candidate "high-safety significant."
- PRA importance measures do not fully address the significance of SSCs that support operator actions for emergency and severe accident management. Such systems can include environmental controls, lighting, alarms, communications, and annunciators. Determination of the categorization of such systems should include consideration of whether the loss of such systems could cause short-term or long-term problems, whether a system failure coincident with an accident is likely, and whether personnel could reasonably compensate for the loss of these support systems.

4.1.3 Identification of Components Which Support Functions

Systems components where QA controls are applied and PRA basic events are different. For example, a diesel failure basic event in the PRA can represent a large number of plant equipment parts including such items as the diesel motor, oil pump, oil cooling fan, motor generator, etc. Other components are not included in PRA basic events because their reliability is assumed to be high enough that their failure probability would have a negligible impact on the CDF and LERF. Therefore, once the high-safety-significant functions in a system for which graded QA is being implemented have been identified, the plant equipment required to support the high-safety-significant functions must be identified independently of the PRA basic event definitions.

An efficient format for this component versus system function identification is a matrix as illustrated in Table 4.1 where the high-safety-significant system functions are listed and cross referenced to all the components needed to support each function at the level of equipment specificity where changes in the application of QA controls will be pursued. The matrix should include all high-safety-significant system functions, all system components which support the high-safety-significant functions, and all external system support functions required by any component. Some examples illustrating areas of

Draft for Comment

Engineering Evaluation

potential concern regarding the accuracy and completeness of the matrix are detailed below. The licensee needs to be able to describe technically how each issue was addressed and resolved.

- A component can directly support another system's function. For example, some containment sump recirculation valves are nominally assigned to the low pressure injection system but directly support containment spray by providing the recirculation flow path.
- Instrumentation used to actuate and control system and plant functions needs careful attention if grading of instrumentation is contemplated. Some instrumentation can belong to one system but provide signals used in other systems, or be used by the operators as a basis for proceduralized or un-proceduralized actions.
- Each system should be reviewed for the possibility of component failures that lead to an initiating event such as loss of feedwater, loss of component cooling water, etc. Components whose failure could cause an initiating event should be identified in the matrix as being required to support the normal operation function (e.g., AOV feedwater control valves are required to support feedwater at power).

The matrix is also needed to systematically propagate safety categorization through successive tiers of support systems not modeled in the PRA. If systems are not graded in a top down sequence, the matrix provides a traceable record of the previously assumed categorization of upper tiered functions requiring support from other systems. Eventually, all support function categorization should be consistent, e.g., the safety significance of the functions requiring support in the upper-tiered system corresponds to the relevant function in the support system.

Table 4.1: Sample Emergency Service Water System Function Versus Component Function Matrix

| COMPONENT | SYSTEM FUNCTIONS | | | REQUIRED COMPONENT SUPPORT |
|-------------|------------------|-----------|--------------------|------------------------------------|
| | Cool DG1A | Cool DG1B | Cool Charging Pump | |
| P-SCC-10A | X | X | X | E.Bus 13 DC Bus 23 ESAF x.x |
| CV-7 | X | X | X | |
| MOV-SCC-165 | | | | E.Bus 13 DC Bus 23 ESAF x.x |
| MV-63 | | | X | |
| HX-14B | | | X | |
| MV-65 | | | X | |
| CV-291 | X | | | |
| HX-E-82A | X | | | |
| AOV-296 | X | | | IA Fun. 5 DC Bus 33 ESAF x.x |

4.1.4 Component Safety Significance Categorization

Selection of the final categorization of system functions and the components which support the high-safety-significant system function is done by integrated assessment of quantitative and qualitative risk insights as described in section 4.3.

The safety significance categorization assigned to components (and to support system functions which can be treated as component functions for initial categorization) is based on the safety significance of the function(s) the component supports. Components which support only low-safety-significant functions should be classified low-safety-significant. The safety significance of components supporting high-safety-significant functions need not always be high, but each such categorization as low-safety significant should be explicitly evaluated and documented and generally done in conformance with licensee defined guidelines. Justification for categorizing a component's safety-significance as low based on high reliability alone will not be acceptable because the high reliability of the component could be a result of the QA program.

4.2 Demonstration of Conformance with Safety Principles

Once the full set of low-safety-significance candidates has been identified, it is necessary to demonstrate that the proposed changes to the QA requirements for these candidates does not violate the safety principles. Guidelines for making that demonstration with due consideration for the scope of the QA program are summarized below. Other equivalent guidelines are acceptable.

The GQA programs need to reflect the multiplicity of current regulations and programs to which some SSCs are subject. For example, some SSCs may need to be excluded from certain reduced QA control categories if those SSCs are also governed by more stringent ASME Code provisions to meet the requirements of 10 CFR 50.55a. In such instances, the ASME Code requirements need to be met.

The engineering evaluation conducted should assess whether the impact of the proposed change is consistent with the principle that sufficient defense-in-depth is maintained. An acceptable set of guidelines for making that assessment is summarized below. Other equivalent decision guidelines are acceptable.

- A reasonable balance among prevention of core damage, prevention of containment failure, and consequence mitigation is preserved.
- Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided.
- System redundancy, independence, and diversity are preserved commensurate with the expected frequency and consequences of challenges to the system (e.g., no risk outliers).
- Defenses against potential common cause failures are preserved and the potential for introduction of new common cause failure mechanisms is assessed.
- Independence of barriers is not degraded.
- Defenses against human errors are preserved.

The engineering evaluation conducted should also assess whether the impact of the proposed change is consistent with the principle that sufficient safety margins are maintained. An acceptable set of guidelines for making that assessment is summarized below. Other equivalent decision guidelines are acceptable.

- Codes and standards or alternatives approved for use by the NRC are met.
- Safety analysis acceptance criteria in the current licensing basis (e.g., FSAR and supporting analysis) are met, or proposed revisions provide sufficient margin to account for analysis and data uncertainty.

The aspects of defense-in-depth and safety margins are expected to be addressed generally by considering the following GQA program aspects:

- The GQA process will not result in changes to the plant configuration. Therefore, no existing plant barriers will be removed. Additionally, existing system redundancy, diversity, and independence will be maintained.
- The GQA process will not result in changes to the technical requirements (e.g., design bases or operational parameters) associated with SSCs.
- The reduced QA controls will be applied only to safety-related SSCs that are determined to be low-safety-significant, and these controls will continue to provide an adequate basis for concluding that the SSCs are expected to perform satisfactorily when called upon to operate.
- The resulting QA provisions will provide the necessary level of assurance that low-safety-significant, safety-related SSCs remain capable of performing their design functions.

The CDF and LERF figures of merit do not fully cover long term containment overpressure protection. Functions credited in the PRA for long term overpressure protection, but which do not contain any SSCs with CDF or LERF based importance measures above the guideline values, should be identified and the safety significance explicitly assigned. For example, the containment spray systems for PWR's may not contribute to the prevention or mitigation of core damage or large early release.

An important factor to ensure that defense-in-depth and safety margin considerations are not degraded during the implementation of graded QA is control of potential common mode failures. As discussed in 4.1.2, groups of nominally identical SSCs, utilized in multiple systems throughout the plant, can as an aggregate have high safety significance. The reduction or loss of independence among components that could be introduced by a reduction of QA controls is not modeled in PRA. Consequently, the licensee should demonstrate that the potential for cross system common mode failures to substantially increase risk is minimized. This assessment is necessary since an underlying assumption in the PRA functional safety-significance determination is that cross system independence exists. Attributes of the QA program that would reduce the likelihood of such vulnerability should be discussed. For example, the graded QA program compensatory measures might include features such as receipt inspection and testing coupled with an appropriate performance monitoring and feedback program. Alternatively, quantitative analyses can be performed to demonstrate that substantial risk increases are minimal.

Principal four in regulatory guide DG-1061 states that any proposed increase in risk is small and does not cause the NRC safety goals to be exceeded. The regulatory guide subsequently defines "small" quantitatively in the form of acceptance guidelines (see section 2.4.2.1 of DG-1061). Although the risk impact of graded QA changes on individual components is expected to be minimal, reduced QA oversight may be applied to a large number of SSCs. It is recognized that limited data is available to define the impact of quality assurance programs on SSC reliability. Accordingly, licensees may choose to provide a qualitative evaluation addressing principal four directly, e.g., that any increase in risk will be small and the safety goals will not be exceeded. Such evaluations should explicitly address the

monitoring and corrective action program. Alternatively, the licensee may use a quantitative evaluation based on, for example, sensitivity studies to demonstrate that the change in CDF and LERF as a result of the implementation of the graded QA program is not expected to exceed the acceptable changes in risk as defined by DG-1061.

4.3 Integrated Assessment

Generally, the performance of, and integration of, the above described evaluations should be performed by a number of technically knowledgeable personnel. One acceptable approach to accomplish this function is to utilize a multi-disciplinary review group of technically proficient plant personnel, referred to here as an expert panel.

If the integrated assessment function is performed by an expert panel, the expert panel determines safety significance and considers QA program adjustments for SSCs categorized as low-safety-significant. The panel would nominally include experienced representatives from various disciplines such as operations, maintenance, engineering, safety analysis and licensing, and PRA. The composition of the expert panel should be augmented, if necessary, to support the purpose of the safety-significance ranking and the grading of QA controls. For example, because of the emphasis on QA considerations in the GQA process, QA and procurement engineering personnel may be assigned to the panel.

The expert panel is responsible for determining the safety significance of the system functions and SSCs. The panel should evaluate both traditional engineering, probabilistic, and qualitative information available regarding the systems and system functions within the defined scope of the graded QA program changes. The evaluation should include either resolving or approving the resolution of the quantitative and qualitative issues addressed in sections 4.1.2.1 and 4.1.2.2.

Safety significance may be determined using guidelines related to prevention and mitigation of core damage, as well as containment integrity and large early release frequency. Factors such as potential common-mode failures, human errors, defense in depth, the importance of plant equipment used for emergency preparedness and plant monitoring functions, and the maintenance of safety margins should also be fully considered. Additional guidance on the integration process is described in Appendix B to the General Standard Review Plan for Risk Informed Regulation.

5. ELEMENT 3: DEVELOP IMPLEMENTATION AND MONITORING STRATEGIES

This section addresses the first, second, third and the fifth principles for risk-informed decision making. The objective of the graded QA effort is to implement a QA program that provides a reasonable level of confidence that plant SSCs will be capable of performing their intended functions. The extent of QA controls will be determined by the relative safety significance and safety functions performed by the equipment to which those controls are applied. The revised licensee's graded QA program will need to specifically identify how the 10 CFR 50, Appendix B criterion will be satisfied. The licensee may adjust the elements of the QA program as it deems necessary to provide a reasonable level of confidence that the SSCs will be capable of performing their intended function. The licensee will demonstrate that the proposed program, in total, is sufficient to achieve this objective.

5.1 Grading of Quality Activities

The first step of the evaluation process is for the licensee to identify specific elements of the quality assurance program controls that will be adjusted for the set of plant equipment that is defined to be low-safety significant. For example, a licensee may propose a change to its verification practices and perform verifications on a sampling basis. Additionally, the licensee should identify the approach for evaluating the adequacy of QA controls for non-safety-related SSCs determined to be high-safety-significant. Augmented quality controls will likely be warranted for these items.

5.1.1 Regulations and Commitments

In accordance with the first principle, no exemptions from current regulations are expected to be needed to implement a graded QA program.

The licensee's QA program description should be revised to address GQA activities applicable to safety-related SSCs of low-safety-significance, including a discussion of how the applicable requirements of Appendix B to 10 CFR Part 50 will be satisfied for that part of the program in accordance with 50.34(b)(6)(ii). This may be accomplished by a discussion that identifies exceptions to applicable NRC regulatory guides (R.S.) and associated endorsed industry standards or by including additional text that describes how Appendix B will be satisfied (merely re-stating the Appendix B provisions will not be acceptable). The submittal should adequately describe the safety significance determination process, and the adjustments made to the QA provisions associated with the eighteen criteria of Appendix B to 10 CFR 50 to describe how the requirements will be satisfied in a graded manner. While considerable flexibility may be exercised, the QA program should be based on standards of performance that are clear, definite, and enforceable.

Grading of QA activities will likely result in changes that reduce QA program commitments relating to SSCs of low-safety-significance. In that event, the NRC would expect the licensee to submit a QA

Draft for Comment

Develop Implementation And Monitoring Strategies

program change to the NRC in accordance with 10 CFR 50.54(a), as discussed further in this section and in section 6.

However, plant SSCs cannot be re-classified as non-safety-related solely based on risk considerations. Regulatory requirements in Appendix A, Section VI(a)(1) of 10 CFR 100, 10 CFR 50.2, 10 CFR 50.49(b)(1), and 10 CFR 50.65(b)(1), prescribe the criteria for determining which SSCs are safety-related and are subject to the provisions of, Appendix B to 10 CFR 50. However, GQA does allow for differences in QA controls for safety-related SSCs based upon their safety significance.

GQA programs should not result in either intended or effective changes in the design, configuration, or technical requirements of plant systems. Such design or configuration changes would occur, for example, when QA program reductions result in a loss of confidence of the SSC's ability to perform its design function. The licensee should ensure that changes to technical requirements are only made in accordance with applicable regulations.

Other regulations, such as the requirements of 10 CFR Part 21 "Reporting of Defects and Noncompliance", including provisions relating to basic components and commercial grade item dedication; 10 CFR Part 50.55(a) "Codes and Standards"; and 10 CFR Part 50.36, "Technical Specifications", remain in effect and may not be changed by means of the GQA program description.

Licensee commitments regarding QA are addressed in a number of documents, including the Final Safety Analysis Report (FSAR), the QA Topical Report, and other docketed correspondence (e.g., responses to generic communications, inspection reports, etc). Licensees are expected to maintain control of their licensing bases. Accordingly, changes from current commitments to QA Regulatory Guides that will be revised as part of the graded QA program should be identified and the manner in which they are being changed should be documented, reviewed, and approved where necessary by the NRC in accordance with 10 CFR 50.54(a), as appropriate.

5.1.2 Grading of Quality Elements

After categorizing the system functions and subsequently the SSCs into two or more safety significance categories as described throughout this Regulatory Guide, the licensee should apply appropriate QA controls for the various categories. This is a critical factor in achieving the goals of the GQA initiative and is performed by an integrated assessment, for example by an expert panel, as discussed in section 4.3.

For safety-related SSCs determined to be high-safety-significant, the current QA practices contained in the NRC approved QA program should be retained.

Licensees have flexibility to define the processes used to achieve reasonable confidence in SSC performance commensurate with their safety significance. Therefore, the licensee may develop reduced, or graded, quality assurance controls for those SSCs assigned to the low-safety-significant category. Example areas where this may be possible are listed in Section 5.2 of this Regulatory Guide.

Draft for Comment

Develop Implementation and Monitoring Strategies

In proposing to reduce controls, two basic objectives should be kept in mind. These are: the GQA program should be sufficient to assure the SSC's design integrity and ability to successfully perform its safety function, and the GQA program should include processes and documentation that support an effective corrective action program as discussed in section 5.3.2. Accordingly, in reducing or enhancing the QA program for any SSC the licensee needs to describe how the proposed changes will achieve the objectives. Also, consideration should be given to issues such as common cause failure issues, as discussed in section 4.2.

A QA program which will identify certain SSCs of low-safety-significance and apply reduced QA requirements to those SSCs should, as a minimum, encompass the four essential elements [as identified in SECY 95-059, "Development of Graded Quality Assurance Methodology"], described in section 1.

It should be emphasized that a certain number of SSCs currently categorized as non-safety-related (i.e., that have not previously been subjected to an Appendix B QA program) may fall into the high-safety-significant category based on application of the methods described in this Regulatory Guide. Licensees should evaluate whether augmented quality assurance practices are warranted for these "high-safety-significant, non-safety-related" SSCs to achieve the above objectives and to fulfill the regulatory requirements of 10CFR50, Appendix A, General Design Criterion 1 which requires that quality programs are to be applied commensurate with the relative importance of SSCs to plant safety. Licensees may voluntarily select certain Appendix B QA program controls as these augmented quality provisions. The use of risk insights should be performed in an integrated manner to identify areas where improvements should be implemented.

The categorization of SSCs as either high safety or low-safety-significant is either derived directly or indirectly from the licensee's PRA, or from qualitative methods that consider the results of PRA where available. In particular, PRA takes credit systematically for non-safety-related SSCs as: 1) providing support to, or 2) alternatives to, and 3) back-ups for safety-related SSCs. Thus, the categorization of safety-related SSCs as low-safety-significant depends upon the proper operation and reliability attributed to non-safety-related SSCs as part of the safety significance determination process. The application of the augmented controls discussed above provides reasonable confidence that the reliability assumed in the risk analysis, or the associated qualitative decision making process, remains valid. The commitment to apply QA controls to high-safety-significant, non-safety-related SSCs, and the delineation of the augmented quality controls that will be applied to those SSCs must be documented by the licensee in the QAP.

5.2 Potential Areas for Implementing Graded QA Program Controls

All 10 CFR Appendix B QA program controls previously applied to low-safety-significant SSCs that are safety-related are candidates for grading subject to the guidance discussed earlier. In addition for high-safety-significant SSCs that are non-safety-related, licensee evaluation should be performed to identify proposed augmented quality controls.

Draft for Comment

Develop Implementation And Monitoring Strategies

Some areas which may be appropriate for applying graded quality assurance program controls for safety-related SSCs of low-safety-significance are discussed below. The list is not exhaustive and licensees may propose graded controls in other areas provided it can be shown the objectives discussed in section 5.1.2 above are met. The goal is to allow licensees flexibility to define acceptable QA controls which provide reasonable confidence that the SSCs will perform their intended functions.

When considering the application of graded QA controls, the licensee should consider the essential elements of the process (such as the safety-significance determination, identification of graded QA controls, associated corrective action methods, and performance monitoring) to be high safety significant activities that are not subject to grading.

5.2.1 Procurement

Licensees may establish less stringent quality assurance requirements for the procurement of low-safety-significant components than for high-safety-significant components. In making these changes, licensees should consider 10 CFR 21 and 10 CFR 50 Appendix B requirements, as implemented by Regulatory Guides 1.44 and 1.123. Within this area, the technical requirements for CGI dedication in accordance with 10 CFR Part 21 (critical characteristics of an item for an application) are not subject to grading. However, for items of low-safety-significance, the verification of critical characteristics may be graded (e.g., by reduced sampling plans, or alternate testing techniques). Other procurement related activities such as auditing, qualifying suppliers, and receipt inspection may also be graded. Licensees should consider the role its procurement practices play in ensuring the prevention of cross-system common cause failures and implement the procurement activities accordingly.

5.2.2 Frequency of Inspections

The licensee may choose to reduce inspection activities related to low-safety-significant SSCs and choose to perform monitoring or surveillance oversight to assure that components can perform their intended functions. Verifications by peer personnel in-lieu of certified inspectors may be implemented for the low-safety-significant SSCs provided that the licensee uses individuals qualified to do inspections and who are independent from the actual performance of the work activity as discussed above. However, these changes cannot conflict with ASME Code required inspections and examinations or other inspections and examinations specified in NRC regulations (e.g., use of the Authorized Nuclear inspector services).

5.2.3 Records and Documentation

Documentation, such as procedures and design packages, for low-safety-significant SSCs may be less detailed than for high-safety-significant items. In assessing the level of detail specified in procedures or actual packages related to low-safety-significant items, there should be enough evidentiary detail to maintain plant design and configuration control. Further, sufficient records need to be maintained to evaluate failures, perform root cause analyses, and to determine appropriate corrective actions. In all

cases and regardless of the risk ranking, a licensee should be able to show that it has sufficient documentation to show that the current facility configuration is consistent with its design bases.

5.2.4 Audits

Processes and work associated with low-safety-significant SSCs may be audited less deeply and less frequently than high-safety-significant activities. Surveillance, performance monitoring, self-assessments, trend data or other activities may in some cases replace formal audits in low-safety-significant areas.

5.2.5 Staff Training and Qualification Requirements

The licensees may establish different training and qualification requirements for personnel performing tasks on low-safety-significant SSCs, however those personnel would need to remain sufficiently technically proficient in their assigned area of responsibility to provide reasonable confidence that affected SSCs would be capable of performing their intended functions. The licensee would need to meet the requirements of the applicable regulations and technical specification requirements pertaining to training programs and staff qualifications.

5.2.6 Corrective Action

Corrective actions are important for all safety-related SSCs and the staff has therefore not identified any portions of the Appendix B corrective action controls which appear to be candidates for grading.

5.3 Performance Monitoring

The implementation of a performance monitoring program is necessary so that the GQA program continues to ensure that component performance is consistent with that assumed in the categorization process. The conduct of performance monitoring is generally addressed in section 2.5 of Reference 25.

As discussed in this regulatory guide, GQA programs do not follow in detail all of the steps inherent in other risk-informed regulatory decision-making applications as outlined in DG-1061, because many of the SSCs of interest in GQA programs are not modeled in the PRAs, and it may not be possible to quantify the effects of changed QA programs on the SSC's performance. For these reasons, a larger portion of the decision-making is left to the discretion and judgement of licensee personnel who perform the integrated assessment function (typically an expert panel).

In the GQA program, the "operational feedback" and "corrective action" portions of the program assume considerable importance in the programs, and their acceptability must be pivotal in the determination of the overall program's acceptability. The licensee should develop criteria for monitoring the performance of the low-safety-significant SSCs based upon risk insights developed during the safety-significance categorization process. The level of the monitoring program (SSC, train,

Develop Implementation And Monitoring Strategies

system, etc.) should provide the capability to determine if, and when, the performance of the low-safety-significant SSCs deteriorates to unacceptably low levels. As QA programs address a broad spectrum of plant activities, the monitoring program should address both plant hardware (SSCs) monitoring as well as process and organizational effectiveness monitoring.

5.3.1 Operational Feedback

The GQA program should include a process (which is generally performed by licensees irrespective of GQA) to evaluate plant and industry operational experience and the potential need to revise SSC safety significance categorizations or QA controls. Operating experience and plant modifications are two sources of information that could give insights about the effectiveness of a licensee's GQA program and feedback mechanisms.

- Operating Experience: Sources of operating experience data include: licensee performance indicators, NRC generic communications, Institute of Nuclear Power Operations (INPO) and Electric Power Research Institute (EPRI) design reliability data, Systematic Assessment of Licensee Performance (SALP) reports, licensee event reports (LERs), NRC inspection reports, equipment maintenance histories, plant performance reviews, reliability and unavailability data, equipment performance or condition trending data, Nuclear Plant Reliability Data System (NPRDS), and quality assurance assessments. The industry-wide data should be evaluated for consistency with PRA assumptions, system unavailabilities, and other plant-specific data.
- Plant Modifications and SSC Replacements: Plant modifications, and SSC replacements and parts thereof, might affect the safety significance determination or selection of QA controls for low-safety-significant SSCs. Accordingly, the GQA program should periodically review plant modifications with respect to their potential impact on safety significance determinations. Alternately, the design change process may include provisions to verify that changes do not affect SSC safety significance or associated QA controls.
- Reliability and Availability Monitoring: The licensee should define performance thresholds based on ensuring, to the extent possible, that the equipment unavailabilities used in the PRA and upon which most of the safety categorization is based remain valid.

A program assessment, which could be accomplished in conjunction with similar Maintenance rule provisions, should be performed to ensure that the overall GQA process (activities associated with safety significance determination, grading of QA controls, implementation of performance monitoring, and application of corrective actions) is being effectively implemented and provide insights into whether the GQA program needs improvements. As part of the assessment, plant deficiencies should be evaluated and the bases for whether the safety significance categorizations (e.g., the PRA model and

assumptions) and assignment of QA controls continue to reflect plant design and operating practices. This assessment should not be performed in a graded manner and should be considered to be a high safety significant activity as it serves to confirm the integrity of the GQA process implementation.

5.3.2 Corrective Actions

The licensee's graded QA program shall include strong and effective corrective action and root-cause analysis, and one of the potential root causes considered should be whether the graded quality assurance treatments of SSCs are sufficient. That is, failures of low-safety-significant SSCs should be identified in accordance with corrective action programs or trending programs so that the licensee can ascertain whether the reduction of the QA controls may have resulted in an unacceptable decrease in an SSC's performance.

Licensee corrective action or trending programs should identify, and determine the apparent cause of failures of SSCs, that meet licensee established thresholds, under the less stringent QA controls to determine if licensee established performance criteria and/or quality elements need to be changed. If the failure is determined to apply generically to other SSCs, or the failure represents a potential common cause concern for similar equipment installed in multiple systems, or if an excessive number of failures occur, then further licensee evaluations are warranted. An apparent cause determination is still warranted to screen the failures in order to ascertain the necessity to perform more in-depth evaluations. The licensee's response to negative performance trends may need to include an assessment of the SSC's safety significance categorization, since the reduction in performance could affect the basis for assigning the SSC to the low-safety-significant category.

The SSC risk-categorization methodology could be potentially affected by the SSC reliability assumptions. This could also potentially affect final categorization decisions to the extent that reliability was used as a licensee criterion for determining the safety significance of the SSC that failed. Both the probabilistic and non-probabilistic methods previously used should be re-evaluated in those instances where there is significant disparity between the analysis assumptions and the observed data. The GQA program controls should be evaluated to determine if they need to be strengthened as a result of the failures. Additionally, based upon performance monitoring results, the licensee may further evaluate both safety-significance categorization and assignment of QA controls to identify situations where they may be relaxed. Such changes would be evaluated as discussed in other sections of this guide.

6. ELEMENT 4: DOCUMENTATION

The recommended format of a plant-specific, risk-informed GQA submittal is presented in this chapter. Use of this format by licensees will help ensure the completeness of the information provided, will assist the NRC staff in locating the information, and will aid in shortening the time needed for the review process. Additional guidance on style, composition, and specifications of safety analysis reports is provided in the Introduction of Revision 3 to Regulatory Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)".

6.1 GQA Program Submittal

The licensee's existing QA program description contained in, or referenced by, the FSAR should be revised to describe the GQA program provisions. The submittal containing the proposed GQA provisions should contain the following:

- (1) the description of the graded QA program implementation scope and the basis for concluding the overall QA program provides reasonable confidence that SSCs remain capable of performing their intended function.
- (2) the process and guidelines developed by the licensee to determine the safety-significance categorization of all SSCs within the Graded QA program scope as defined in this regulatory guide.
- (3) the role of the staff who perform the integrated assessment function (expert panel).
- (4) the process for determining the QA controls being applied to each safety-significance category of SSCs.
- (5) a description of the adjustments proposed as part of the GQA program and how the requirements of each of the criterion of Appendix B to 10 CFR 50 will be satisfied in a graded manner.
- (6) augmented QA controls for non-safety related SSCs categorized as high-safety-significant.
- (7) important assumptions including SSC functional capabilities and performance attributes, which play a key role in supporting the acceptability of the QA program change. Since continued satisfaction of these assumptions is necessary to maintain the validity of the categorization process, these licensee commitments will need to be reflected in the QAP description of the change.
- (8) the operational feedback and enhanced corrective action mechanisms and processes to adjust both safety significance categorization of SSCs and the associated QA controls.

- (9) the performance monitoring process, and SSC functional performance and availability attributes which form the basis of the proposed change.

6.2 Plant Data and Engineering Evaluation

Licensees may submit the following information as a separate document to support the proposed GQA submittal. This information should be available for staff review at the licensee's offices.

6.2.1 Systems Pertinent to GQA

Summarize design and operating features of systems where changes to the QA program are planned, and systems supported by the systems where changes to the QA program are planned. For each system, include a table summarizing key design and operating data. Values that are used in the analysis should be identified and justified. Refer to appendices or other documents (e.g., specific sections of the FSAR or design bases documents) as necessary for more details. Systems to be considered should include the pertinent portions of all systems modeled in the plant-specific probabilistic analysis.

6.2.2 Status of SSCs

All SSCs whose QA program control is proposed to be changed should be listed in a table which should include (at a minimum) the plant's SSC label, the current QA categorization (by default all safety-related SSCs will initially have a "high" QA categorization), the proposed QA categorization, associated correlation with system functions, and a brief explanation of the justification for the proposed change.

6.2.3 Plant Operating Experience

Summarize any major events involving failures whose occurrence was attributable to inadequate or improperly applied QA controls at this plant. Include in this summary any lessons learned from these events and indicate actions taken to prevent or minimize recurrence of the events.

6.2.4 Engineering Evaluation

In addition to the general documentation requirements identified in Reference 25, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis ", provide justification of the plant's continued compliance with applicable rules and regulations, and provide a complete description of each issue considered for the engineering evaluation and a discussion of how the resolution of each issue impacts the categorization of SSCs. All information should be provided in the main report.

Documentation should also be available describing the methods and techniques used for developing quantitative and qualitative risk insights used to support the categorization the safety significance of

SSCs. All risk studies used should be clearly identified, including the date and the version of the studies as applicable. Other documentation should include a description of;

- (1) the review process whereby the risk studies, the findings of the review process, and the licensees response to any questions or comments raised by the reviewers.
- (2) how the importance measures were calculated and used (including the guidelines to categorize if applicable). This information should be augmented by technical description on how the limitations associated with the use of importance measures discussed in Chapter 4.1.2.1 were resolved.

General guidance on acceptable documentation for the content and quality of risk studies used to support a risk informed application can be found in Reference 25, "An approach for using probabilistic risk assessment in Risk-informed decisions on plant-specific changes to the current licensing basis," DG-1061.

7. REFERENCES

1. 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants."
2. 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants."
3. 10 CFR Part 50, 50.55a, "Codes and Standards."
4. 10 CFR Part 50, 50.55(e), "Conditions of Construction Permits"(reporting significant QA deficiencies).
5. 10 CFR Part 50, 50.34(b.6.ii), "Contents of Application; Technical Information" (Final Safety Analysis QA program description).
6. 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants."
7. Regulatory Guide 1.8, "Personnel Selection and Training" (endorses ANSI/ANS 3.1).
8. Regulatory Guide 1.26, "Quality Group Classification, and Standards for Water, Steam, and Radioactive Waste Containing Components of Nuclear Power Plants."
9. Regulatory Guide 1.28, "Quality Assurance Program Requirements (Design and Construction)" (endorses N45.2).
10. Regulatory Guide 1.29, "Seismic Design Classification."
11. Regulatory Guide 1.30, "Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment" (endorses N45.2.4).
12. Regulatory Guide 1.37, "Quality Assurance Requirements for Cleaning of Fluid Systems and Associated Components of Water-Cooled Nuclear Power Plants" (endorses N45.2.1).
13. Regulatory Guide 1.38, "Quality Assurance Requirements for Packaging, Shipping, Receiving, Storage, and Handling of Items for Water-Cooled Nuclear Power Plants" (endorses N45.2.2).
14. Regulatory Guide 1.39, "Housekeeping Requirements for Water-Cooled Nuclear Power Plants" (endorses N45.2.3).
15. Regulatory Guide 1.58, "Qualification of Nuclear Power Plant Inspection, Examination, and Testing Personnel" (endorses N45.2.6).
16. Regulatory Guide 1.64, "Quality Assurance Requirements for the Design of Nuclear Power Plants" (endorses N45.2.11).

Draft for Comment

References

17. Regulatory Guide 1.74, "Quality Assurance Terms and Definitions" (endorses N45.2.10).
18. Regulatory Guide 1.88, "Collection, Storage, and Maintenance of Nuclear Power Plant Quality Assurance Records" (endorses N45.2.9).
19. Regulatory Guide 1.94, "Quality Assurance Requirements for Installation, Inspection, and Testing of Structural Concrete and Structural Steel During the Construction Phase of Nuclear Power Plants" (endorses N45.2.5).
20. Regulatory Guide 1.116, "Quality Assurance Requirements for Installation, Inspection, and Testing of Mechanical Equipment and Systems" (endorses N45.2.8).
21. Regulatory Guide 1.123, "Quality Assurance Requirements for Control of Procurement of Items and Services for Nuclear Power Plants" (endorses N45.2.13).
22. Regulatory Guide 1.144, "Auditing of Quality Assurance programs for Nuclear Power Plants" (endorses N45.2.12).
23. Regulatory Guide 1.146, "Qualification of Quality Assurance Program Audit Personnel for Nuclear Power Plants" (endorses N45.2.23).
24. Branch Technical Position (BTP) ASB 9.5-1 (attached to SRP Section 9.5.1).
25. Regulatory Guide DG-1061, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis".
26. SECY-95-059, "Development of Graded Quality Assurance Methodology", March 10, 1995.
27. NUREG-1602 (Draft), "Use of PRA in Risk-Informed Applications".
28. Memorandum from Suzanne Black (NRR/HQMB) to William Beckner (NRR/PDIV-1) and William Bateman (NRR/PDIV-2), "Letters to Volunteer Licensees Participating in Graded Quality Assurance Initiative", January 24, 1996.
29. EPRI TR-105396, "PSA Applications Guide", August, 1995.
30. NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants", Revision 0.
31. Reg Guide 1.160, "Monitoring The Effectiveness of Maintenance At Nuclear Power Plants".



**U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY
RESEARCH**

DRAFT REGULATORY GUIDE

Contact: H. W. (Roy) Woods (301)415-6622

**AN APPROACH FOR PLANT-SPECIFIC, RISK-INFORMED
DECISIONMAKING: TECHNICAL SPECIFICATIONS**

DG-1065, REV. 6

MARCH 13, 1997

DRAFT FOR COMMENT

This regulatory guide is being issued in draft form to involve the public in the early stages of the development of a regulatory position in this area. It has not received complete staff review and does not represent an official NRC staff position.

Public comments are being elicited on the draft guide (including any implementation schedule) and its associated regulatory analysis or value/impact statement. Comments should be accompanied by appropriate supporting data. Written comments may be submitted to the Rules Review and Directives Branch, DFIPS, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555. Copies of comments received may be examined at the NRC Public Document Room, 2120 L Street NW., Washington, DC. Comments will be most helpful if received by

Requests for single copies of draft or active regulatory guides (which may be reproduced) or for placement on an automatic distribution list for single copies of future draft guides in specific divisions should be made in writing to the U.S. Nuclear Regulatory Commission, Washington, DC 20555, Attention: Distribution and Mail Services Section, or by fax to (301)415-2260.

CONTENTS

| | Page |
|---|------|
| 1. INTRODUCTION | 1-1 |
| 1.1 Background | 1-1 |
| 1.2 Purpose and this Regulatory Guide | 1-2 |
| 1.3 Scope of this Regulatory Guide | 1-2 |
| 1.4 Relationship to Other Guidance Documents | 1-2 |
| 2. AN ACCEPTABLE APPROACH TO RISK-INFORMED DECISIONMAKING REGARDING TS CHANGES | 2-1 |
| 3. ELEMENT 1: DEFINE THE PROPOSED CHANGE | 3-1 |
| 3.1 Reason for Proposed Change | 3-1 |
| 3.1.1 Improvement in Operational Safety | 3-1 |
| 3.1.2 Consistency of Risk Basis in Regulatory Requirements | 3-1 |
| 3.1.3 Reduce Unnecessary Burdens | 3-1 |
| 4. ELEMENT 2: CONDUCT ENGINEERING EVALUATIONS | 4-1 |
| 4.1 Compliance With Current Regulations | 4-1 |
| 4.2 Traditional Engineering Considerations | 4-1 |
| 4.2.1 Maintenance of Defense-in-Depth | 4-1 |
| 4.2.2 Maintenance of Safety Margins | 4-3 |
| 4.2.3 Additional Engineering Considerations | 4-4 |
| 4.3 Evaluation of Risk Impact | 4-4 |
| 4.3.1 Quality of the PRA | 4-6 |
| 4.3.2 Scope of the PRA for TS Change Evaluations | 4-6 |
| 4.3.3 PRA Modeling | 4-7 |
| 4.3.3.1 Detail Needed for TS Changes | 4-7 |
| 4.3.3.2 Modeling of Initiating Events | 4-10 |
| 4.3.3.3 Screening Criteria | 4-11 |
| 4.3.3.4 Truncation Limits | 4-11 |
| 4.3.4 Assumptions in AOT and STI Evaluations | 4-12 |
| 4.3.5 Sensitivity and Uncertainty Analyses Relating to Assumptions in TS Change Evaluations | 4-15 |
| 4.3.6 Use of Compensatory Measures in TS Change Evaluations | 4-16 |
| 4.3.7 Contemporaneous Configuration Control | 4-16 |
| Acceptance Guidelines for TS Changes | 4-17 |
| 4.4 Comparison of Risk of Available Alternatives | 4-19 |
| 4.6 Cumulative Effect of TS Changes | 4-19 |
| 5. ELEMENT 3: DEVELOP IMPLEMENTATION AND MONITORING PROGRAM | 5-1 |
| 5.1 Three-Tiered Implementation Approach | 5-1 |
| 5.2 Maintenance Rule Control | 5-1 |
| 6. ELEMENT 4: SUBMIT PROPOSED CHANGE | 6-1 |
| 7. BIBLIOGRAPHY | 7-1 |
| A. APPENDIX A - OTHER CONSIDERATIONS AND DATA NEEDS IN TS CHANGE RISK EVALUATIONS | A-1 |
| A.1 Other Considerations in TS Change Risk Evaluations | A-1 |
| A.1.1 Risk Measures for TS Changes to AOTs and STIs | A-1 |
| A.1.2 Measures for Multiple TS Changes | A-2 |
| A.1.2.1 Measures That Can Be Combined for Multiple TS Changes | A-2 |
| A.1.2.2 Total Impact of Multiple Changes | A-3 |
| A.1.3 Quantification of Risk Measures | A-3 |
| A.1.3.1 Alternative Ways of Calculating TS Change Risk Measures | A-3 |

| | | |
|-------|--|------|
| | A.1.3.3 Treatment of CCF and Recovery Factors | A-7 |
| | A.1.3.4 Calculations of Transition Risk | A-8 |
| A.2 | Data Needs for TS Change Evaluations | A-8 |
| A.2.1 | Care in Using Plant-Specific Data | A-8 |
| A.2.2 | Considerations When Generic Data Are Used | A-9 |
| A.2.3 | Specific Data Needs | A-9 |
| | A.2.3.1 Maintenance-Downtime Data | A-9 |
| | A.2.3.2 Maintenance Schedules and Frequency | A-10 |
| | A.2.3.3 Data Relating to Component Testing | A-10 |
| | A.2.3.4 Parameters for Component Unavailability | A-10 |
| | A.2.3.5 Separating Demand and Standby Time Contributions to Unavailability | A-11 |
| | A.2.3.6 Test-Caused Transients | A-12 |
| | A.2.3.7 Data for Evaluating Transition Risk | A-12 |

FIGURE

Page

| | | |
|-----|---|-----|
| 2.1 | General Description of an Acceptable Approach to Risk-Informed Applications | 2-3 |
|-----|---|-----|

1. INTRODUCTION

1.1 Background

Section 182a of the *Atomic Energy Act* requires that applicants for nuclear power plant operating licenses shall state:

[S]uch technical specifications, including information of the amount, kind, and source of special nuclear material required, the place of the use, the specific characteristics of the facility, and such other information as the Commission may, by rule or regulation, deem necessary in order to enable it to find that the utilization . . . of special nuclear material will be in accord with the common defense and security and will provide adequate protection to the health and safety of the public. Such technical specifications shall be a part of any license issued.

In 10 CFR 50.36, the Commission established its regulatory requirements related to the content of technical specifications (TS). In doing this, the Commission placed emphasis on those matters related to the prevention of accidents and the mitigation of accident consequences; the Commission noted that applicants were expected to incorporate into their TS "those items that are directly related to maintaining the integrity of the physical barriers designed to contain radioactivity" (33 FR 18610). Pursuant to 10 CFR 50.36, TS are required to contain items in the following five specific categories: (1) safety limits, limiting safety system settings, and limiting control settings; (2) limiting conditions for operation; (3) surveillance requirements; (4) design features; and (5) administrative controls.

Since the mid-1980s, the NRC has been reviewing and granting improvements to TS based, at least in part, on probabilistic risk assessment (PRA) insights. Some of these improvements have been proposed by the NSSS owners groups to apply to an entire class of plants. Many others have been proposed by individual licensees. Typically, the proposed improvements involved a relaxation of one or more allowed outage times (AOTs) or surveillance test intervals (STIs) in the TS.

In its July 22, 1993 final policy statement on TS improvements, the Commission stated that it:

...expects that licensees, in preparing their Technical Specification related submittals, will utilize any plant-specific PSA or risk survey and any available literature on risk insights and PSAs . . . Similarly, the NRC staff will also employ risk insights and PSAs in evaluating Technical Specifications related submittals. Further, as a part of the Commission's ongoing program of improving Technical Specifications, it will continue to consider methods to make better use of risk and reliability information for defining future generic Technical Specification requirements.

The Commission reiterated this point when it issued the revision to 10 CFR 50.36 in July 1995.

DRAFT FOR COMMENT

Risk-informed TS submittals primarily deal with permanent changes to TS requirements, i.e., as the name suggests, the requirement is permanently changed when approved, and is applicable to all future occurrences. A one-time change to a TS requirement, where a different requirement is requested for a particular incident, also can use risk-informed evaluations, but it involves slightly different scope and considerations. This regulatory guide focuses on permanent changes to TS.

1.2 Purpose and this Regulatory Guide

This regulatory guide describes an acceptable approach for applying risk-informed methods to the changing of nuclear power plant TS allowed outage times (AOTs) and surveillance test intervals (STIs) in order to assess the impact of such proposed changes on the risk associated with plant operation in a consistent manner.

1.3 Scope of this Regulatory Guide

This regulatory guide describes an acceptable approach for assessing the nature and impact of proposed permanent TS changes in AOTs and STIs by considering engineering issues and applying risk insights. Assessments should consider relevant safety margins and defense-in-depth attributes, including consideration of success criteria as well as equipment functionality, reliability and availability. Acceptance guidelines for evaluating the results of such evaluations are provided also.

This regulatory guide also describes development of acceptable TS change implementation strategies and performance monitoring plans that are sensitive to uncertainties.

Finally, this regulatory guide indicates an acceptable level of documentation that will enable the staff to reach a finding that the licensee has performed a complete and scrutable TS change analysis and that the results of the engineering evaluations support the licensee's request for the TS change.

1.4 Relationship to Other Guidance Documents

This regulatory guide does not duplicate material in Regulatory Guide DG-1601, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis," which should be consulted for topics common to all risk-informed regulatory applications. Additionally, the companion draft NUREG-1602, "Use of PRA in Risk-Informed Applications," contains reference material on issues and methods for PRA that can be used to support regulatory decisionmaking. This regulatory guide provides only that guidance needed specifically for risk-informed TS changes over and above that given in Regulatory Guide DG-1061.

2. AN ACCEPTABLE APPROACH TO RISK-INFORMED DECISIONMAKING REGARDING TS CHANGES

This Regulatory Guide describes a four-element approach (illustrated in Figure 2.1) for evaluating risk-informed TS changes that encompasses each of the following five key principles of the staff's philosophy of risk-informed decisionmaking applied to TS changes.

1. **The proposed change meets the current regulations.** Applicable rules and regulations that form the regulatory basis for TS are discussed in Section 4.1, "Compliance with Current Regulations".
2. **Defense-in-depth is maintained.** The guidance contained in Section 4.2, "Traditional Engineering Considerations", applies the various aspects of maintaining defense-in-depth to the subject of changes in TS.
3. **Sufficient safety margins are maintained.** The guidance contained in Section 4.2, "Traditional Engineering Considerations", applies various aspects of maintaining sufficient safety margin to the subject of changes to TS.
4. **Proposed changes in risk, both individual and cumulative, are small or are reductions and should not cause the NRC Safety Goals to be exceeded.**
5. **Performance-based implementation and monitoring strategies are proposed that address uncertainties in analysis models and data and provide for timely feedback and corrective action.** The three-tiered implementation approach discussed in Section 5.1, and Maintenance Rule control discussed in Section 5.2 provide guidance in meeting this principle.

Given the principles of risk-informed decisionmaking discussed above, the staff expects that a certain evaluation approach and acceptance guidelines that follow from those principles will be followed by licensees in implementing these principles, and the staff has identified a four-element approach to evaluating proposed CLB changes, as described in regulatory guide DG-1061, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis," December 1997. Those detailed discussions regarding the evaluation approach and acceptance guidelines are not repeated here; instead, specific application of the four-element approach for risk-informed TS is discussed.

Element 1: Define the proposed TS change

The licensee needs to explicitly identify the particular technical specifications that are affected by the proposed change, and identify available engineering studies, methods, codes, and PRA studies that are related to the proposed change. The licensee should consider how such changes will affect conformance

with the plant's current licensing basis (CLB)¹. The licensee should also determine how the affected systems, components, or parameters are modeled in the PRA and should identify all elements of the PRA that the change impacts. The licensee should utilize PRA insights to both determine the impact of the change on plant safety and to understand the impact on the licensing basis. Chapter 3 describes element 1 in more detail.

Element 2: Conduct engineering evaluations

The licensee should examine the proposed change to verify that it meets existing applicable rules and regulations. In addition, the licensee should determine how the change impacts defense in depth aspects of the plant's design and operation, and should determine the adequacy of safety margins following the proposed change. Finally, the licensee should consider how plant and industry operating experience relates to the proposed change, and what potential compensatory measures could be taken to offset any negative impact from the proposed change.

The licensee should also perform risk-informed evaluations of the proposed change to determine the impact on plant risk. The evaluation should explicitly consider the specific plant equipment affected by the proposed TS changes and the effects of the proposed change on the functionality, reliability, and availability of the affected equipment. The necessary scope and level of detail of the analysis depends upon the particular systems and functions that are affected, and it is recognized that there will be cases for which a qualitative, rather than quantitative, risk analysis is acceptable.

The licensee should provide the rationale that supports the acceptability of the proposed changes by integrating probabilistic insights with traditional considerations to arrive at final determination of risk. The determination should consider the continued conformance to existing applicable rules and regulations, the adequacy of the traditional engineering evaluation of the proposed change, and the change in plant risk relative to the acceptance guidelines. All of these areas should be adequately addressed before the change is considered acceptable. The specific guidance for an acceptable approach for performing engineering evaluations of changes to TS is found in Chapter 4.

¹ This regulatory guide adopts the 10 CFR Part 54 definition of current licensing basis. That is, "Current Licensing Basis (CLB) is the set of NRC requirements applicable to a specific plant and a licensee's written commitments for ensuring compliance with and operation with in applicable NRC requirements and the plant-specific design basis (including all modifications and additions to such commitments over the life of the license) that are docketed and in effect. The CLB includes the NRC regulations contained in 10 CFR Parts 2, 19, 20, 21, 26, 30, 40, 51, 54, 55, 70, 72, 73, 100 and appendices thereto; orders; license conditions; exemptions; and technical specifications. It also includes the plant-specific design-basis information defined in 10 CFR 50.2 as documented in the most recent final safety analysis report (FSAR) as required by 10 CFR 50.71 and the licensee's commitments remaining in effect that were made in docketed licensing correspondence such as licensee responses to NRC bulletins, generic letters, and enforcement actions, as well as licensee commitments documented in NRC safety evaluations or licensee event reports."

DRAFT FOR COMMENT

Element 3: Develop implementation and monitoring program

The licensee should develop an implementation and performance monitoring program formulated to confirm the assumptions and analyses that were conducted to justify the CLB change, to ensure that plant operational safety can be maintained consistent with the assumptions in the PRA analysis of Element 2, and to ensure that the process provides criteria for taking actions based on the results of the monitoring efforts. Specific guidance for element 3 is provided in Chapter 5.

Element 4: Submit proposed change

The final element involves documenting the analyses and submitting the license amendment request. NRC will review the submittal according to NRC Standard Review Plan (SRP) Chapter 16.X, "Risk-Informed Decisionmaking: Technical Specifications", and in accordance with the NRC regulations governing license amendments (10 CFR 50.90, 50.91, and 50.92). Documentation and submittal guidance for risk-informed TS change evaluations are provided in Chapter 5 of this regulatory guide.

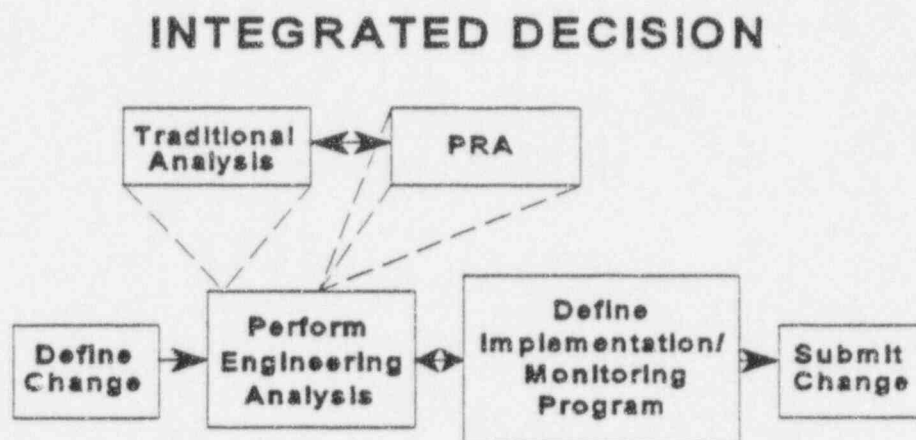


Figure 2.1 General description of an acceptable approach to risk-informed applications.

3. ELEMENT 1: DEFINE THE PROPOSED CHANGE

3.1 Reason for Proposed Change

The reasons for requesting the TS change or changes should be stated in the submittal along with information that demonstrates that the extent of the change is needed. Generally acceptable reasons for requesting TS modifications fall into one or more of the categories below.

3.1.1 Improvement in Operational Safety

The reason for the TS modification may be to improve operational safety; that is, a reduction in the plant risk or a reduction in occupational exposure of plant personnel in complying with the requirements.

3.1.2 Consistency of Risk Basis in Regulatory Requirements

The TS modifications requested can be supported on their risk implications. TS requirements can be changed to reflect improved design features in a plant or to reflect equipment reliability improvements that make a previous requirement unnecessarily stringent or ineffective. TS may be changed to establish consistently based requirements across the industry or across an industry group. It must be ensured that the risk resulting from the change remains acceptable.

3.1.3 Reduce Unnecessary Burdens

The change may be needed to reduce unnecessary burdens in complying with current TS requirements, based on the operating history of the plant or industry in general. For example, in specific instances, the repair time needed may be longer than the AOT defined in the TS. The required surveillance may lead to plant transients, result in unnecessary equipment wear, result in excessive radiation exposure to plant personnel, or place unnecessary administrative burdens on plant personnel that are not justified by the safety significance of the surveillance requirement. In some cases, the change may provide operational flexibility, and, in those cases, the modification might allow an increase in the allocation of the plant personnel's time to more safety-significant aspects.

4. ELEMENT 2: CONDUCT ENGINEERING EVALUATIONS

The second element of an acceptable approach to risk-informed TS modifications involves assessing the impact of the proposed TS change on postulated design basis accidents and transients and on potential core damage accidents, using both traditional engineering methods and PRA techniques and insights.

Licensees are expected to provide strong technical bases for any TS change. The technical bases should be rooted in traditional engineering and system analyses. TS change requests based on PRA results alone should not be submitted for review. TS change requests should give proper attention to the integration of considerations such as conformance to Standard Technical Specifications, generic applicability of the requested change if it is different from Standard Technical Specifications, operational constraints, manufacturer recommendations, and practical considerations for test and maintenance. Standard practices used in setting AOTs and STIs should be followed, e.g., AOTs nominally used are 8 hours, 12 hours, 24 hours, 72 hours, 7 days, 14 days, etc. STIs nominally used are 12 hours, 7 days, 1 month, 3 months, etc. Using such standards greatly simplifies implementation, scheduling, monitoring, and auditing. Logical consistency among the requirements should be maintained, e.g., AOT requirements for multiple trains out of service should not be longer than that for one of the constituent trains.

4.1 Compliance With Current Regulations

In evaluating proposed changes to TS, the licensee must ensure that the current regulations are met, consistent with principle #1 of risk-informed regulation. The NRC regulations specific to TS are stated in 10 CFR 50.36, "Technical Specifications." Additional information with regard to the NRC's policies on TS is contained in the "NRC Final Policy Statement on Technical Specification Improvements for Nuclear Power Reactors" (58 FR 39132). These documents define the main elements of TS and provide criteria for items to be included in the TS. The final policy statement and the statement of considerations for 10 CFR 50.36 (60FR36953) also discuss use of probabilistic approaches to improve TS. Regulations regarding application for and issuance of license amendments are found in 10 CFR 50.90, 50.91, and 50.92. In addition, the licensee should ensure that the TS change does not result in non-compliance with any other portion of the current licensing basis.

4.2 Traditional Engineering Considerations

4.2.1 Maintenance of Defense-in-Depth

One aspect of the engineering evaluations is to show that the fundamental safety principles on which the plant design was based are not compromised. Design basis accidents (DBAs) play a central role in nuclear power plant design. DBAs are a combination of postulated challenges and failure events against which plants are designed and design features that ensure adequate and safe plant response. During the design process, plant response and associated safety margins are evaluated using assumptions which are intended

to be conservative. National standards and other considerations such as defense-in-depth attributes and the single failure criterion constitute additional engineering considerations that influence plant design and operation. Margins and defenses associated with these considerations may be affected by the licensee's proposed TS change and, therefore, should be reevaluated to support a requested TS change. As part of this evaluation, the impact of the proposed TS change on affected equipment functionality, reliability, and availability will be determined.

The licensee should assess whether the proposed TS change meets the defense-in-depth principle (principle #2). Defense-in-depth consists of a number of elements as summarized below. These elements can be used as guidelines for making that assessment. Other equivalent acceptance guidelines are acceptable.

- Defense-in-depth is maintained:

- a reasonable balance among prevention of core damage, prevention of containment failure, and consequence mitigation is preserved, e.g., the proposed change in a TS AOT or STI has not significantly changed the balance among these principles of prevention and mitigation. TS change requests should consider whether the anticipated operational changes associated with a change in an AOT or STI could introduce new accidents or transients or could increase the likelihood of an accident or transient
- over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided, e.g., a programmatic configuration control process should not be relied upon to account for a large risk increase associated with a TS AOT extension
- system redundancy, independence, and diversity are maintained commensurate with the expected frequency and consequences of challenges to the system, e.g. there are no risk outliers (the following items should be considered):
 - there are appropriate restrictions in place to preclude simultaneous equipment outages that would erode the principles of redundancy and diversity;
 - compensatory actions to be taken when entering the extended AOT from pre-planned maintenance are identified;
 - voluntary removal of equipment from service during plant operation should not be scheduled when adverse weather conditions are predicted or at times when the plant may be subjected to other abnormal conditions; and
 - the impact of the TS change on the safety function should be taken into consideration. For example, what is the impact of a change in the AOT for the low pressure safety injection system on the overall availability and reliability of the low pressure injection function?

DRAFT FOR COMMENT

Engineering Evaluation

- defenses against potential common cause failures are maintained and the potential for introduction of new common cause failure mechanisms is assessed, e.g., TS change requests should consider whether the anticipated operational changes associated with a change in an AOT or STI could introduce any new common cause failure modes not previously considered
- independence of barriers is not degraded, e.g., TS change requests should address the licensee's overall configuration risk management system which will provide a means of ensuring that the independence of barriers has not been degraded by the TS change
- defenses against human errors are maintained, e.g., TS change requests should consider whether the anticipated operation changes associated with a change in an AOT or STI could change the expected operator response or introduce any new human errors not previously considered.

4.2.2 Maintenance of Safety Margins

The engineering evaluation conducted should assess whether the impact of the proposed TS change is consistent with the principle that sufficient safety margins are maintained (principle #3). An acceptable set of guidelines for making that assessment are summarized below. Other equivalent decision guidelines are acceptable.

- Sufficient safety margins are maintained:
 - codes and standards or alternatives approved for use by the NRC are met, e.g., the proposed TS AOT or STI change is not in conflict with approved codes and standards relevant to the subject system
 - safety analysis acceptance criteria in the FSAR are met, or proposed revisions provide sufficient margin to account for analysis and data uncertainties, e.g., the proposed TS AOT or STI change does not adversely affect any assumptions or inputs to the safety analysis, or, if such inputs are affected, justification is provided to ensure sufficient safety margin will continue to exist. For TS AOT changes, an assessment should be made of the effect on the FSAR acceptance criteria assuming the plant is in the AOT (i.e., the subject equipment is inoperable), and there are no additional failures. Such an assessment should result in the identification of all situations where entry into the proposed AOT could result in failure to meet an intended safety function.

4.2.3 Additional Engineering Considerations

Additional considerations that are unique to risk-informed TS changes should be taken into account in an engineering evaluation. These items can be summarized as follows:

- (1) TS AOT and STI modifications should be supported by the overall safety benefit.
- (2) Justification for TS AOT modifications should be based on the need for extended equipment outage time and the demonstrated availability of redundant equipment. The AOT defined should be adequate to complete the majority of the component repairs or post-maintenance activities intended to be performed during power operation; however, AOTs should not be based solely on preventative maintenance activities that require long outage times but occur infrequently (e.g., once every five years). In addition, the AOT should be adequate to conduct any required surveillance tests that render the component or system inoperable. The burden of testing and maintenance can place a stress on the crew, which can affect the quality of the testing or maintenance and thereby the component reliability. Crew burden should be part of the consideration in deciding changes to requirements.
- (3) Regardless of the AOT, the actual time equipment is removed from service should be minimized. The removal should be performed during stable plant conditions and should not result in repeated TS entries.
- (4) TS change requests should consider both plant-specific and industry-wide operational experience on systems important for coping with transients or accidents.
- (5) Some systems may not be modeled by the plant's PRA, but could affect the best estimate of the performance or availability of systems that might provide a backup function for the system for which the TS change is being requested (this could change the required performance or availability of the system for which the TS change is being sought). The review should, therefore, consider systems beyond those modeled in the PRA.
- (6) TS change requests should consider the occupational exposure to test and maintenance personnel to conduct required test and maintenance on the subject TS system.

4.3 Evaluation of Risk Impact

The staff has identified a three-tiered approach for licensees to evaluate the risk associated with proposed TS AOT changes. The first tier is an evaluation of the impact on plant risk of the proposed TS change as expressed by the change in core damage frequency (ΔCDF), the change in the incremental conditional core

DRAFT FOR COMMENT

Engineering Evaluation

damage probability (ICCDP)², and the incremental conditional large early release probability (ICLERP). The second tier is an evaluation of the process used to address potentially high risk configurations that could exist if equipment in addition to that associated with the change were to be taken out of service simultaneously, or other risk significant operational factors such as concurrent system or equipment testing were also involved. The objective of this part of the review is to ensure that appropriate restrictions on dominant risk-significant configurations associated with the change are in place. The third tier is an evaluation of the overall configuration risk management system to ensure that adequate programs and procedures are in place to identify and compensate for other potentially lower probability, but nonetheless risk-significant configurations resulting from maintenance and other operational activities. Although defense in depth is protected to some degree by most current TS, the three-tiered approach to the evaluation of risk-informed TS modifications discussed in the following section provides additional assurance that defense in depth will not be significantly impacted by such changes to the licensing basis.

Tier 1: PRA Capability and Insights

In the first tier, the licensee should assess the impact of the proposed TS modification on core damage frequency (CDF), ICCDP, and ICLERP. To support this assessment, two aspects need to be considered: 1) the validity of the PRA, and 2) the PRA insights and findings. The licensee should demonstrate that its PRA is valid for assessing the proposed TS modifications and identify the impact of the TS change on plant risk.

Tier 2: Avoidance of Risk-Significant Plant Configurations

The licensee should also provide reasonable assurance that risk-significant plant equipment outage configurations will not occur when specific plant equipment is out of service consistent with the proposed TS modification. An effective way to perform such an assessment is to evaluate systems and/or components according to their contribution to plant risk (or safety) while the plant is in a limiting condition for operation (LCO) for equipment AOT. Once system equipment is so evaluated, an assessment can be made as to whether certain enhancements to the TS, or procedures, are needed to avoid risk-significant plant configurations. In addition, compensatory actions which can mitigate any corresponding increase in risk (e.g., backup equipment, increased surveillance frequency, or upgrading procedures and training) should be identified and evaluated. Any changes made to the plant design or operating procedures as a result of such a risk evaluation (required backup equipment, increased surveillance frequency, or upgraded procedures and training required before certain plant system configurations can be entered) should be incorporated into the analyses utilized for TS modifications as described under "Tier 1" above.

²ICCDP = [(conditional CDF with the subject equipment out of service) - (baseline CDF with nominal expected equipment unavailabilities)] X (duration of single AOT under consideration).

Tier 3: Risk-Informed Plant Configuration Control and Management

In the third tier, the licensee focuses on programs that ensure that the risk impact of out-of-service equipment is appropriately evaluated prior to performing any maintenance activity. A viable program would be one that is able to uncover risk-significant plant equipment outage configurations as they evolve during real-time, normal plant operation. This can be accomplished by quantitatively evaluating the impact on plant risk of equipment unavailability, operational activities like testing or load dispatching, or weather conditions. The need for this third tier stems from the difficulty of identifying all possible risk-significant configurations under Tier 2. Tier 2 programs typically result in a table or set of tables that assume certain systems are unavailable, and specify other systems that cannot be out of service under the assumed conditions. This third tier is needed because of the difficulty of providing a set of tables under Tier 2 that cover all plant configurations that will ever be encountered over extended periods of plant operation.

Sections 4.3.1 through 4.3.7 and Appendix A discuss various issues related to the three-tiered approach described above. In general, Sections 4.3.2 through 4.3.5 and Appendix A outline issues associated with Tier 1, and Sections 4.3.6 and 4.3.7 outline issues associated with Tiers 2 and 3, respectively.

There may be situations where a non-quantitative assessment of risk (either alone or accompanied by quantitative assessment) is sufficient to justify TS changes. The licensee is expected to use its judgment of the acceptability (to support regulatory decisionmaking) of the risk argument being considered, including the appropriate blend of quantitative and qualitative assessments.

4.3.1 Quality of the PRA

The quality of the PRA must be compatible with the safety implications of the TS change being requested. That is, the more the potential change in risk and/or the greater the uncertainty in that risk due to the requested TS change, the more rigor that must go into ensuring the quality of the PRA. The licensee should ensure that the quality of the PRA is compatible with its intended use. DG-1061 provides guidance regarding the expected quality of PRAs for risk-informed regulatory applications, including TS. With regard to TS in particular, it should be noted that some licensees may elect to use the PRA underlying their individual plant examination (IPE) to analyze the risk impact associated with requested TS changes. The NRC staff's review of the IPE submittal alone does not suffice as an adequate review for TS applications.

4.3.2 Scope of the PRA for TS Change Evaluations

The scope and the level of PRA necessary to support the evaluation of a TS change depend on the type of TS change being sought. To define the needed scope, a full-power, internal-event PRA is first considered, and other aspects (e.g., operating modes, types of events, Level 2) are added as needed.

The level of PRA that should be conducted depends on the type of TS change involved. Minimally, for systems used to prevent core damage (i.e., most of the TS systems modeled in a PRA other than the containment systems), Level 1 evaluations should be performed. For containment systems, Level 2 evaluations are likely to be needed at least to the point of assessing containment structural performance.

Engineering Evaluation

When only a Level 1 PRA is available but additional Level 2 information is desirable, one acceptable method for approximating the needed information is defined in DG-1061, Appendix B.

For modifications to TS requirements defined for the power operation mode, full-power internal-event PRAs, for which the scope includes internal fires and flooding, should be used. When modifications to requirements for systems needed for decay heat removal are considered, then an assessment of shutdown risk should also be considered. Examples of such systems are auxiliary feedwater, residual heat removal, emergency diesel generator, and service water. Also, when AOTs are being modified to facilitate online maintenance (that is, transferring scheduled preventive maintenance (PM) from shutdown to power operation), the impact on the shutdown modes should also be evaluated. Using both power operation and shutdown models, a comparative evaluation may be presented to decide the appropriate condition for scheduling maintenance based on risk evaluations.

When AOTs are being modified in anticipation of the need for additional time for corrective maintenance, then an assessment of transition risk which could be incurred under the current, shorter AOT is also desirable. Also, TS changes to requirements for a controlled shutdown (i.e., the time allocated to transit through hot standby to hot shutdown to cold shutdown, or to the final state that should be reached) should be evaluated using a model for the transition risk covering these periods.

4.3.3 PRA Modeling

4.3.3.1 Detail Needed for TS Changes

To evaluate a TS change, the specific systems or components involved should be modeled in the PRA. The model should also be able to treat the alignments of components during periods when testing and maintenance are being carried out.

Typically, LCOs and surveillance requirements (SRs) relate to the system trains or components and are modeled in the system fault trees of a PRA. System fault trees should be sufficiently detailed to specifically include all the components for which surveillance tests and maintenance are performed and are to be evaluated.

- For AOT evaluations, system train-level models are adequate as long as all components belonging to the train are clearly identified (i.e., the failure of all those components that cause the train to fail). In using train-level models, common-cause contributions must be adequately treated.
- For evaluating STIs, individual component-level models are necessary.

Since, typically, PRAs are done at the component level, they are directly used to analyze both AOTs and STIs.

Component unavailability models should include significant contributions from random failure, common-cause failure (CCF), test downtime, and maintenance downtime.

- The component unavailability model for test downtime and maintenance downtime should be based on a realistic estimate of expected surveillance and maintenance practices after the TS change is approved and implemented, e.g., how often the AOT is expected to be entered for preplanned maintenance or surveillance.
- The component unavailability model for test downtime and maintenance downtime should also be based on plant-specific and industry-wide operating experience.
- The component unavailability model for test downtime and maintenance downtime should be developed with consideration for an appropriate balance between prevention of failures of the subject system or component through maintenance and minimizing unavailability of the system or component due to testing or maintenance.
- The component unavailability model should have the flexibility to separate contributions from test and maintenance downtime. For evaluating an AOT, the contribution from maintenance downtime can be equated to zero to delete it. For an STI evaluation, the contribution from test downtime determines a contribution to risk from carrying out the test.
- Additional details in terms of separating the failure rate contributions into cyclic demand-related and standby time-related contributions can be incorporated, if justifiable, for evaluating surveillance requirements.

The CCF contributions should be modeled so that they can be modified to reflect the condition in which one or more of the components is unavailable. It should be noted, however, that CCF modeling of components is not only dependent on the number of remaining in-service components, but is also dependent on the reason components were removed from service, i.e., whether for preventive or corrective maintenance. For appropriate configuration risk management and control, preventive and corrective maintenance activities need to be considered. Tier 3 PRA models should, therefore, have the ability to address the subtle difference that exists between maintenance activities.

To account for the effects of test placements for redundant components in relation to each other (e.g., staggered or sequential test strategy), time-dependent models and additional evaluations using specialized codes may be needed. Time-dependent evaluations can be made using system fault-tree models to decide on the test strategy for the redundant components in the system. The corresponding system unavailability can be used to determine the core damage frequency.

If the PRA does not model the system for which the TS change is being requested, then certain limits should apply for requesting changes to the TS for these systems. Examples of these situations are given below:

DRAFT FOR COMMENT

Engineering Evaluation

- (1) When a system is modeled in the event tree, but a detailed fault tree model is not provided (direct estimate of system unavailability from experience data or expert judgment is used), then the TS evaluation can proceed in one of two ways:
 - (a) a separate fault tree can be developed for the system for TS evaluation and used to complement the existing PKA model without directly modifying the PRA, or
 - (b) a bounding evaluation can be conducted based on impact of system failures that are modeled in the PRA event trees; that is, failure of any component in the system can be assumed to cause system failure.
- (2) When a separate fault tree is developed, then specific TS requirements within the system can be changed, and changes in the system unavailability can be measured which can then be used in the PRA model to obtain the corresponding Level 1 and Level 2/3 measures, as appropriate. Such evaluations can be considered similarly as those evaluations made directly using PRA models, but should satisfy the following conditions:
 - (a) failures within the system should not affect any other system/component failure;
 - (b) the effect of system failure should not influence any initiating event frequency (or it should have a minimal/negligible effect); or
 - (c) the system should not share components with another system.
- (3) When bounding evaluations are performed assuming any failure in the system as a system failure, then the calculated risk impacts for TS changes are expected to be overestimated. The corresponding changes that may be acceptable will also be fewer than those that could have been justified using a detailed model. When considering the incorporation of non-PRA factors, this perspective should be kept, while at the same time considering the lack of a detailed model. Here also, the above three conditions discussed for the previous case apply.
- (4) When a TS change is being considered for a system in which some of the components in the system have been modeled as part of other system components, but detailed system modeling was not done (such systems are not expected to be modeled in the event tree), the risk impact of the TS changes can then be evaluated on the basis of this limited modeling. The risk impact of the TS changes can be underestimated for the following reasons:
 - (a) additional components may be affected by the failure of the components, and that failure may not have been considered; or
 - (b) CCF of redundant components may not have been considered.

Usually, the most risk-important components have been modeled and other components in the system are the same or lower in the risk-importance ranking. When making judgments on the TS requirements for the components in the system based on another component that has been modeled, an evaluation should be performed to ensure that the impact of its failure is not greater than the component which is being used as its surrogate.

In these cases, since the risk-informed evaluation will be limited, and as discussed, some overestimation of the risk may have been incorporated, then non-risk related, engineering considerations gain importance in the overall decision. In such cases, arguments for the change also must be for very small increments from current requirements.

4.3.3.2 Modeling of Initiating Events

Some initiating events resulting from support system failure (e.g., service water, component cooling water, instrument air) are modeled explicitly in the logic model, i.e., fault tree models are developed in the PRA. Any TS change for these systems will affect the corresponding initiating event frequency as well as the system unavailability. The effect of TS changes on these initiating event frequencies should be considered.

Some test and maintenance activities can contribute to some transients. Initiating-event frequencies used in the PRA do not separate out this contribution. Such a separation may be needed during TS change evaluations. For example, the effect of test-caused transients may be evaluated in deciding an STI. Initiating-event frequencies from conduct of the test (i.e., test-caused transients) are modeled separately to evaluate the risk contribution from test-caused transients. Data needs for estimating initiating event frequencies from test-caused transients are discussed in section A.2 of the appendix.

4.3.3.3 Screening Criteria

The main qualitative consideration regarding the screening of sequences in TS change evaluations is the inclusion of sequences directly affected by the TS change that would have been truncated by frequency-based screening alone. For example, if the TS change involves accumulators in a pressurized-water reactor (PWR), qualitative considerations imply that sequences that contain the accumulators should be included, even if these sequences do not meet the frequency criteria. Excluding these sequences would result in an underestimate of the risk impact of the TS changes.

4.3.3.4 Truncation Limits

Truncation levels should be appropriately used to ensure that underestimation, due to truncation of cutsets, does not occur. Additional precautions, as discussed below, are needed to avoid truncation errors in calculating risk measures.

When failure or outage of a single component is considered, as in the case of an AOT or STI risk evaluation, the truncation levels in evaluating R_i and R_o are of concern. $[R_i]$ is the increased CDF, with the

Engineering Evaluation

component assumed to be inoperable (or equivalently the component unavailability set to "true"), and R_o is the reduced CDF, with the component assumed to be operable (or equivalently, the component unavailability set to "false"). If cutsets generated in the base case PRA are used to calculate R_i and R_o , then it first has to be ensured that the component in question appears in the cutsets being used. If the component in question appears in the cutsets near the truncation limit (e.g., all appearances are in cutsets within a factor of 10 of the truncation limit), it may be necessary to reduce the truncation limit. If R_i is marginally larger than the base case value, then one order of additional cutsets should be generated to ensure that any underestimation did not take place. Typically, a truncation level set below the base case CDF by an amount that corresponds to the basic event unavailability for the component in question can be considered adequate; that is, consider that a plant base case CDF of 10^{-6} and R_i is being calculated for a component whose unavailability is 10^{-3} , then cutsets up to 10^{-9} may be adequate. Cutsets should be regenerated for selected cases to ensure that the truncation level being used is adequate.

When risk from plant configurations involving multiple components is being considered, a cutset with a relatively small frequency can become a significant contributor to the CDF. This is because more than one of the affected components may appear in the same minimal cutset, and if the availability of more than one of these components is decreased by the TS change, this can cause a significant increase in the cutset's frequency. For such cases, truncation levels have to be reduced by an amount corresponding to the product of the unavailabilities of the components involved in the outage configuration, to ensure that the base case's cutsets can be used.

4.3.4 Assumptions in AOT and STI Evaluations

Using PRAs to evaluate TS changes requires consideration of a number of assumptions made within the PRA which can have a significant influence on the ultimate acceptability of the proposed changes. Such assumptions should be discussed in the submittal requesting the TS changes.

Assumptions that should be considered for AOT change evaluations can be summarized as follows:

- (1) AOT risk evaluations are usually performed using the PRA for power operation (i.e., to calculate the risk associated with (a) the equipment being unavailable during power operation for the duration of the AOT and (b) any change in the AOT). The risk associated with shutting the plant down because of AOT violations usually is not considered. In most cases, this risk is considered negligible, or such consideration is assumed to further justify the requested change. For some situations (e.g., for residual heat removal systems, service water systems, and auxiliary feedwater systems), comparative risk evaluations of continued power operation vs. plant shutdown should be considered.
- (2) When calculating the risk impacts (i.e., a change in CDF due to AOT changes), the change in average CDF should be estimated using the mean outage times for the current and proposed AOTs. Usually, data for outage times correspond to the current AOT, but not to the proposed AOT. Different assumptions are made to estimate the outage time corresponding to the proposed AOT. Usually, the assumption used implies that the same policy of repairing a failed component will remain in effect

when the AOT extension is granted, as will the waiting period to start a repair, and the number of maintenance personnel engaged in a repair.

- (3) When the risk impact of an AOT change is evaluated, the yearly risk impact that is calculated takes into account the outage frequency. An AOT extension may imply that the maintenance of the component is improved, which may reduce the component's failure rate, and consequently, the frequency of outages needed for correcting degradations or failure. Again, there are no experience data for the extended AOT; therefore, the assumption should be made that both the frequency of outage for corrective maintenance and the component's failure rate remain the same. Here, the beneficial aspect of maintenance is not quantified and this may give a slightly higher estimate of the yearly AOT risk measure for the proposed AOT.
- (4) Often, AOT extensions are requested to facilitate on-line (or at-power) preventive maintenance of safety-system components. Their frequency and duration may be estimated and the risk impact due to the resulting unavailability of such equipment can be calculated.
- (5) When AOTs of multiple safety system trains are extended, the likelihood of simultaneous outages of multiple components increases (resulting from combinations of failures, testing, and maintenances) because the increased duration increases the probability of the individual events which constitute the simultaneous multiple outages; hence, overlapping of routinely scheduled activities and random failures becomes more likely. The impact of such occurrences on the average plant risk, e.g., CDF, is small, but the conditional risk can be large. This issue is addressed as part of the implementation considerations (see Sections 4.3.7 and 6.1).

Assumptions that should be considered for STI evaluations can be summarized as follows:

- (1) Surveillance tests usually are assumed to detect failures that have occurred in the standby period. The component failure rate λ , in the formulation of component unavailability, represents these failures. In estimating the test-limited risk, it usually is assumed that a surveillance test of a component detects the failures, and that after the test, the component's unavailability resets to zero or "false" in the Boolean expression. A few component failures, depending on a component's design and the test performed, may not be detected by a routine surveillance test. Usually, their contribution to risk is considered negligible.
- (2) Regular surveillance testing of a component, as performed for safety-system components, is considered to influence its performance. Generally, for most components, the increase of a surveillance interval beyond a certain value may reduce the component's performance (i.e., increase the failure rate). Experience data are not available to assess the STI values beyond which the component failure rate λ increases. In a risk-informed evaluation of surveillance requirements, the failure rate is assumed to remain the same (i.e., unaffected by a change in the test interval). This assumption implies that the STIs are not being changed beyond the value where λ may be affected. Care should be taken not to extend the STIs beyond such values using risk-informed analyses only.

Engineering Evaluation

- (3) The timing of surveillance tests for redundant components relative to each other (i.e., the test strategy used) has an impact on the risk measures calculated. Staggered or sequential test strategies are commonly used. In most PRAs, no specific test strategy is modeled; tests are assumed to be conducted independently at specified intervals. Separate system-level time-dependent evaluations should be carried out to evaluate the effect of different test strategies where it can impact the evaluation of the change being considered.
- (4) Notwithstanding the beneficial aspects of testing to detect failures that occur in a standby period, a number of adverse effects may be associated with the test: downtime to conduct the test, errors of restoration after the test, test-caused transients, and test-caused wear of the equipment. Downtime and errors of restoration are usually modeled in a PRA, unless they are negligible. Test-caused transients and wear of the equipment are applicable to a few tests, but they are not generally modeled separately in a PRA. However, they can be evaluated using PRA models supplemented with additional data and analysis. Methods are available to quantitatively address these aspects; however, qualitative arguments can also be presented to support the extension of a test interval. Where the adverse impact of testing is considered significant, such cases should preferably be addressed quantitatively.

4.3.5 Sensitivity and Uncertainty Analyses Relating to Assumptions in TS Change Evaluations

As in any risk-informed study, risk-informed analyses of TS changes can be affected by numerous uncertainties regarding the assumptions made during the PRA model's development and application.

Sensitivity analyses will be necessary to address the important assumptions in the submittal made with respect to TS change analyses. They should include:

- impact of variation in repair/maintenance policy due to AOT changes (e.g., scheduling a PM of longer duration at power).
- impact of variation in assumed mean downtimes or frequencies.
- effect of separating the cyclic demand vs. standby time-related contribution to the component's unavailability in deciding changes to an STI.
- effect of details regarding how CCFs are modeled in the PRA.

Sensitivity analyses performed previously for risk-informed TS changes have shown that the risk resulting from TS AOT changes is relatively insensitive to uncertainties (compared to the effect on risk due to uncertainties in assumptions regarding plant design changes, or regarding significant changes to plant operating procedures, for examples). Licensees are expected to justify any deviations from this expectation. This is because the uncertainties associated with AOT changes tend to similarly affect the base case (i.e., before the change) and the changed case (i.e., with the change in place). That is, the risks

result from similar causes in both cases (i.e., no new initiating transients or subsequent failure modes are likely to have been introduced by relatively minor AOT changes). AOT changes subject the plant to a variation in its exposure to the same type of risk, and the PRA model is able to predict, with relative surety based on data from operating experience, how much that risk will change based on that changed exposure. Similar results are expected for STI changes.

The above argument may be more difficult to justify in cases where the effects of multiple outages may become significant during relatively large increases in AOTs or STIs. In those cases, however, the Tier 2 and Tier 3 aspects of TS changes (i.e., configuration monitoring, risk predictions, and configuration control based on the risk predictions) are expected to be robust and will be relied upon to control the resulting potential for significant risk increases.

4.3.6 Use of Compensatory Measures in TS Change Evaluations

Consistent with the fundamental principle that changes to TS result in very small increases in the risk to the health and safety of the public (principle #4, as described in Section 2.4.2.1 of DG-1061), as part of proposed TS change evaluations, certain compensatory measures (discussed below) that balance the calculated risk increase due to the changes may be considered. This consideration should be made in light of the acceptance guidelines given in DG-1061. Also, note that these considerations may be part of Tier 2 or Tier 3 programs.

When the licensee wishes to reduce the risk increase resulting from a proposed change even though the individual change is judged by the licensee to meet the "very small" guideline, the licensee might consider taking compensatory measures such as those suggested below. These compensatory measures can be acceptable if they are proposed and evaluated as part of the overall application for the TS change. However, compensatory measures should not be relied upon to compensate for weaknesses in plant design. Compensatory measures included in the submittal for a TS change should be measures not already included in the current licensing basis, but which would become part of the licensing basis if the TS change were approved. Examples of compensatory measures are:

- adding a test of a redundant train before initiating a scheduled maintenance activity as part of an AOT extension
- limiting simultaneous testing and maintenance of redundant or diverse systems as part of an AOT extension
- incorporating a staggered test strategy as part of STI extension
- improving test and maintenance procedures to reduce test and maintenance related errors
- improving operating procedures and operator training to reduce the impact of human errors
- improving system designs, which reduces overall system unavailability and plant risk

When compensatory measures are part of the TS change evaluation, then the risk impact of these measures should be considered and presented, either quantitatively or qualitatively. When a quantitative evaluation is used, the total impact of these measures should be evaluated by comparison to the "very small" guideline (principle #4, as described in Section 2.4.2.1 of DG-1061). This includes:

DRAFT FOR COMMENT

Engineering Evaluation

- (1) evaluation of the proposed TS changes without the compensatory measures
- (2) evaluation of the proposed TS changes with the compensatory measures
- (3) specific discussion of how each of the compensatory measures is credited in the PRA model or during the evaluation process

4.3.7 Contemporaneous Configuration Control

Consistent with the fundamental principle that changes to TS result in very small increases in the risk to the health and safety of the public (principle #4, as described in Section 2.4.2.1 of DG-1061), certain configuration controls need to be utilized. The need for the controls discussed in this section is described at the beginning of Section 4.4 in the discussion regarding Tier 3.

Licensees should describe their capability to perform a contemporaneous assessment of the overall impact on safety of proposed plant configurations prior to performing and during performance of maintenance activities which remove equipment from service. Licensees should explain how these tools or other processes will be used to ensure that risk-significant plant configurations will not be entered and that appropriate actions will be taken when unforeseen events put the plant in a risk-significant configuration.

The staff has determined that the Technical Specifications Administrative Controls section should describe the licensee's program for performing a real-time assessment as described above and that the Bases for TS for which an extended AOT is granted should reference this program description. The following items should be addressed in such a configuration control program:

- a. The assessment applies prior to entering an LCO for pre-planned maintenance activities and while in an LCO to perform either preventive or corrective maintenance activities.
- b. The assessment is a risk-informed assessment using the current version of the licensee's PRA and reflects the as-built, as-operated plant.
- c. The assessment looks at the real-time or contemporaneous plant configuration.
- d. The purpose of the assessment is to assess the overall impact on plant risk and to take any actions necessary to minimize risk.
- e. The process for performing the assessment is documented in plant procedures.
- f. The capability and validity of the real-time PRA configuration control process, if different from the PRA used to assess the AOT extensions.
- g. Containment (PRA Level 2) concerns and external events are considered.

Each submittal for a risk-informed TS AOT extension should contain appropriate changes to the Administrative Control section which incorporate description of a program incorporating these items.

4.4 Acceptance Guidelines for TS Changes

The guidelines discussed in Sections 2.4.2.1 and 2.4.2.2 of DG-1061 are applicable to TS AOT and STI change requests. Numerical acceptance guidelines are presented in those subsections as a function of the result of the licensee's risk analysis in terms of total CDF predicted for the plant and the change in CDF and LERF predicted for the TS change(s) requested by the licensee. In addition, those sections discuss cases where the scope of the licensee's PRA does not include a Level 2 (containment performance) analysis, and where, according to the guidelines presented in this regulatory guide and in DG-1061, such an analysis is needed. Application of those guidelines to individual proposals for TS modifications will be done in a manner consistent with the fundamental principle that changes to TS result in very small increases in the risk to the health and safety of the public (principle #4, as described in Section 2.4.2.1 of DG-1061).

TS change evaluations may involve some very small increase in risk as quantified by PRA models. Usually, it is argued that such a very small increase is offset by the many beneficial effects of the change that are not modeled by the PRA. The role of numerical guidelines is to ensure that the increase in risk is very small, and to provide a quantitative basis for the risk increase based on aspects of the TS change that are modeled or quantified.

The numerical guidelines used to decide an acceptable TS change are taken into account along with other traditional considerations, operating experience, lessons learned from previous changes, and practical considerations associated with test and maintenance practices. The final acceptability of the proposed change should be based on all of these considerations and not solely on the use of PRA-informed results compared to numerical acceptance guidelines.

As discussed previously, the numerical guidelines are used to ensure that any increase in risk is within acceptable limits; traditional considerations are used to ensure that the change satisfies rules and regulations which are in effect; practical considerations judge the acceptability of implementing the change; and lessons learned from past experience ensure that mistakes are not repeated.

Using the risk measures discussed in this regulatory guide, the increase in risk should be calculated for the TS changes and compared against the numeric guidelines referenced above in this subsection. In calculating the risk impact of the changed case, additional changes to be implemented as part of the change can be credited. For example, in seeking an STI change, if the test strategy is also to be changed, the effect of this should also be incorporated in the risk evaluation.

However, it should be noted that this TS-specific regulatory guide, as well as DG-1061, are applicable only to permanent (as opposed to temporary, or "one time") changes to TS requirements. TS AOT changes are permanent changes, but, because AOTs are entered infrequently and are temporary by their

Engineering Evaluation

very nature, the following TS-specific acceptance guidelines are provided in addition to those given in DG-1061. That is:

1. The licensee has demonstrated that the TS AOT modification has only a very small quantitative impact on plant risk. An ICCDP of less than $5.0E-7$ is considered very small for a single TS-AOT modification. An ICLERP of $5.0E-8$ or less is also considered very small. Also, the ICCDP contribution should be distributed in time such that any increase in the associated instantaneous risk is very small and within the normal operating background (risk fluctuations) of the plant (Tier 1).
2. The licensee has demonstrated that there are appropriate restrictions on dominant risk-significant configurations associated with the modification (Tier 2).
3. The licensee has implemented a risk-informed plant configuration control program. The licensee has implemented procedures to utilize, maintain, and control such a program (Tier 3).

4.5 Comparison of Risk of Available Alternatives

In some cases, in support of a TS modification, available alternatives are compared to justify the TS change. For changes in TS AOTs, such cases primarily involve comparing the risk of shutting down with the risk of continuing power operation, given that the plant is not meeting one or more TS LCOs. Such comparisons can be used to justify that the increase in at-power risk associated with the TS change is offset by the averting of some transition or shutdown risk.

In the case of an STI change, the beneficial and adverse impacts can be similarly compared. The modified STI should be chosen so that the benefit of testing is at least equal to, or greater than, the adverse effects of testing. For example, if the calibration of relays in the reactor protection system causes plant transients, the risk from the test-caused transients is then estimated and compared with the test-limited risk of an extended STI.

In using such guidelines, the following considerations apply:

- (1) The uncertainty associated with the two measures being compared can differ, and should be considered in deciding on an acceptable change
- (2) When the risk measures associated with all alternatives are unacceptably large, ways to reduce the risk should be explored, instead of only extending the TS requirement. That is, a large risk from one of the alternatives should not be the justification for TS relaxation without giving appropriate attention to risk-reduction options. If the risk from test-caused transients is large, attention may then be given to exploring changes in test procedures to reduce such risk, rather than only extending the test interval. However, a combination of the two also may be appropriate.

4.6 Cumulative Effect of TS Changes

The cumulative impact of the proposed TS changes should be calculated and presented, in addition to the individual impacts. The total, cumulative impact is estimated using the average value of the risk measures. The conditional measures, i.e., CDP and LERP, do not directly apply in evaluating the total impact from multiple changes. As discussed earlier, conditional measures are used in deciding changes to individual requirements.

In presenting the cumulative risk impact, the base case PRA model should be used consistently. It should not contain any of the proposed changes, but should reflect any other recent changes to the plant. The same model used for evaluating the individual changes should be used for assessing cumulative impact. Plant practices proposed for implementation as part of the TS changes should not be credited in the base case.

Previously approved TS changes also should be discussed as part of the cumulative impact evaluation. When the base case PRA model has been updated incorporating the previously approved TS changes, then it should be so stated. If the base case does not include previously approved changes, they should then be included as part of the cumulative impact evaluation of the proposed changes.

5. ELEMENT 3: DEVELOP IMPLEMENTATION AND MONITORING PROGRAM

5.1 Three-Tiered Implementation Approach

As described in Section 4.3, the staff expects licensee to use a three-tiered approach in evaluating the risk associated with proposed TS changes. Application of the three-tiered approach is in keeping with the fundamental principle that performance-based implementation and monitoring strategies be employed to account for uncertainties in analysis models and data (principle #5). Because of such uncertainties, these methods are used to avoid, or severely limit, the time durations during which plant operation is allowed with high-risk configurations of plant equipment (i.e., with excessive unavailability of critical safety equipment).

5.2 Maintenance Rule Control

In order to ensure that extension of a TS AOT or STI does not degrade operational safety over time, the licensee should ensure performance monitoring mechanisms are in place to identify negative trends in availability or reliability of equipment impacted by TS changes. As part of implementing the maintenance rule (10 CFR 50.65), each licensee will likely have developed target goals for the majority of TS equipment, which could provide such a performance monitoring mechanism. The effect of TS changes should be considered if any adverse trends in meeting established goals are identified through implementation of the maintenance rule. If the licensee concludes that the performance or condition of a TS system or component affected by a TS change does not meet established goals, appropriate corrective action shall be taken to reverse the trend, in accordance with the maintenance rule. Such corrective action may include submittal of another TS change to shorten the revised AOT or STI, if the licensee determines this is an important factor in reversing the negative trend.

6. ELEMENT 4: SUBMIT PROPOSED CHANGE

The evaluations performed to justify the proposed TS changes should be documented and included in the license amendment request submittal. Regulatory Guide DG-1061 provides guidance on acceptable documentation and submittal materials to support risk-informed decisionmaking. Specifically, documentation to support risk-informed TS change requests should include:

- (1) A description of the TS changes being proposed and the reasons for seeking the changes,
- (2) A description of the process used to arrive at the proposed changes,
- (3) Traditional engineering evaluations performed,
- (4) Changes made to the PRA for use in the TS change evaluation,
- (5) Review of the applicability and quality of the PRA models for TS evaluations,
- (6) Discussion of the risk measures used in evaluating the changes,
- (7) Data additional to the plant's PRA database developed and used,
- (8) Summary of the risk measures calculated including intermediate results,
- (9) Sensitivity and uncertainty analyses performed,
- (10) Summary of the risk impacts of the proposed changes and any compensating actions proposed
- (11) A tabulation of equipment outage configurations that could threaten the integrity of important safety functions and that are prohibited by TS or plant procedures (Tier 2).
- (12) A description of the capability to perform a contemporaneous assessment of the overall impact on safety of proposed plant configurations including an explanation of how these tools will be used to ensure that risk-significant plant configurations will not be entered and that appropriate actions will be taken when unforeseen events put the plant in a risk-significant configuration (Tier 3).
- (13) A marked up copy of the relevant TS and Bases. The level of detail provided in the TS Bases should include adequate information to provide the technical basis for the revised AOT or STI.
- (14) All other documentation required to be submitted with a license amendment request.

7. BIBLIOGRAPHY

Atomic Safety and Licensing Appeal Board, *Portland General Electric Company*. (Trojan Nuclear Plant), ALAB-531, 9 NRC 263 (1979).

Codes of Federal Regulations, Title 10, "Energy":

10 CFR 50.36, "Technical Specifications."

10 CFR 50.90 "Application for amendment of license or construction permit."

10 CFR 50.91 "Notice for public comment; State consultation."

10 CFR 50.92 "Issuance of amendment."

U.S. Nuclear Regulatory Commission, 33 FR 18612, Statement of Considerations, "Technical Specifications for Facility Licensees; Safety Analyses Reports," *Federal Register*, December 17, 1968.

U.S. Nuclear Regulatory Commission, 58 FR 39132, "Final Policy Statement on Technical Specifications Improvements for Nuclear Power Reactors," *Federal Register*, July 22, 1993

U.S. Nuclear Regulatory Commission, Final Rule, 10 CFR 50.36, 60 FR 36953, "Technical Specifications," *Federal Register*, July 19, 1995.

U.S. Nuclear Regulatory Commission, NUREG-0800, Chapter 16.X, "Standard Review Plan for Risk-Informed Decisionmaking: Technical Specifications", December 1997.

NUREG-1430, "Standard Technical Specifications, Babcock and Wilcox Plants" (latest revision).

NUREG-1431, "Standard Technical Specifications, Westinghouse Plants" (latest revision)

NUREG-1432, "Standard Technical Specifications, Combustion Engineering Plants"(latest revision).

NUREG-1433, "Standard Technical Specifications, General Electric Plants, BWR/4" (latest revision)

NUREG-1434, "Standard Technical Specifications, General Electric Plants, BWR/6" (latest revision).

NUREG-1602, Draft, "Use of PRA in Risk-Informed Applications", October 1996.

U.S. Nuclear Regulatory Commission, NUREG-CR-6141, "Handbook of Methods for Risk-Based Analyses of Technical Specifications," November 1994

Electric Power Research Institute TR-105867, "Guidelines for Preparing Risk-Based Technical Specifications Change Request Submittals," December 1995.

DRAFT FOR COMMENT

Electric Power Research Institute TR-105987, "Template for the Submission of Revised Risk-Based Technical Specifications," December 1995.

U.S. Nuclear Regulatory Commission Regulatory Guide DG-1061, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis", December 1997.

U.S. Nuclear Regulatory Commission, NUREG-0800, Chapter 19.0, "Standard Review Plan for Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decisionmaking: General Guidance", December 1997.

A. APPENDIX A - OTHER CONSIDERATIONS AND DATA NEEDS IN TS CHANGE RISK EVALUATIONS

A.1 Other Considerations in TS Change Risk Evaluations

A.1.1 Risk Measures for TS Changes to AOTs and STIs

In this section, a list of the risk-informed measures used in AOT and STI evaluations is presented. A more detailed discussion of these measures can be found in NUREG/CR-6141, "Handbook of Methods for Risk-Based Analyses of Technical Specifications."

The measures applicable for AOT evaluations are:

- conditional risk given the LCO
- single-event AOT risk
- yearly AOT risk

When comparing the risk of shutting down with the risk of continuing power operation for a given LCO, the applicable measures are:

- risk of continued power operation for a given downtime,
similar to single-event AOT risk
- risk of shutting down for the same downtime

The measures applicable for STI evaluations are:

- test-limited risk
- test-caused risk

Similar to the AOT evaluations, the risk contributions associated with preventive maintenance (PM) are:

- single PM risk
- yearly PM risk

The risk associated with simultaneous outages of multiple components, called configuration risk, is calculated as part of AOT changes. The three-tier approach discussed at the beginning of this Section 4 includes calculations of risks associated with multiple components that may be taken down together. The applicable measures are similar to the AOT measures stated above:

- conditional risk (e.g., CDF) caused by the configuration
- increase in risk, [e.g., CDP (obtained by multiplying the increase in CDF by the duration of the configuration for the occurrence of a given configuration)].

A.1.2 Measures for Multiple TS Changes

When multiple TS changes are being considered, then the combined impact of the changes should be considered, in addition to the individual impacts. The considerations relating to the calculation of total impacts are discussed here.

A.1.2.1 Measures That Can Be Combined for Multiple TS Changes

When considering risk contributions from several AOTs, the risk measures can be combined according to the following guidelines:

The single-event AOT risks from several AOTs do not generally interact nor do they accumulate to give a total contribution because the single AOT risks are conditional risks per event, and the downtime events for the different AOTs are different events. The only time that single-event AOT risks need to be simultaneously considered is when multiple components can be down at the same time, constituting the same event. Such a case is referred to as "downed configuration," or simply a "configuration." The risk contribution associated with a configuration is referred to as the configuration risk, and is evaluated separately as a multiple component downtime. Conducting maintenance on several components is a principal cause of potentially high configuration risks.

Yearly AOT risk contributions from several AOTs can interact and need to be accumulated to give the total yearly contribution from all the AOTs being considered. When the AOTs do not interact, that is, when the downed components are not in the same minimal cutset, the yearly AOT risk contribution from several AOTs is then the sum of the individual yearly AOT risk contributions. When the AOTs do interact, that is, when two or more of the downed components are in the same minimal cutset, interaction of the AOT risk contributions then needs to be considered.

When calculating the test-limited risk for changes in multiple STIs, the total test-limited risk then needs to be properly evaluated. Simple addition of individual test-limited risks will not provide the combined test-limited risk. In a simple addition, the total test-limited risk contribution is underestimated because the interacting terms are neglected.

A.1.2.2 Total Impact of Multiple Changes

When multiple changes are requested, the total collective risk impact from all the changes then needs to be evaluated. For example, for a group of AOT and STI changes, this includes the total impact of all the requested:

- AOT changes
- STI changes
- AOT and STI changes

If multiple changes are made, the impact of each change is assessed individually, then as a check, the plant PRA should be used to quantify the total impact.

A.1.3 Quantification of Risk Measures

A.1.3.1 Alternative Ways of Calculating TS Change Risk Measures

In calculating the measures discussed for evaluating TS changes, two specific risk levels are discussed, which need to be quantified using a PRA. Focusing on the CDF level, they are: R_1 , the increased risk level (e.g., CDF) with the component assumed down or equivalent component unavailability set to "true," and R_0 , the reduced CDF with the component assumed up; that is, the component unavailability is set to "false."

Using PRA To Obtain AOT, PM, and Configuration Risk Contributions

R_1 can be calculated by setting the component-down event to a true state in the PRA. Similarly, R_0 can be calculated by setting the component-down event to a false state in the PRA. The component-down event in the PRA is the event describing that the component is down for repair or maintenance. If the component-down event is included in the existing minimal cutsets, then these minimal cutsets can be used to determine R_1 and R_0 provided the minimal cutsets sufficiently cover the contribution of the down event. The existing minimal cutsets are sufficient if those containing the down event are not all near the truncation limit (i.e., are not all within a factor of 10 of the truncation limit). Alternatively, the minimal cutsets are sufficient if those containing the down event have a non-negligible contribution (i.e., have a contribution greater than or equal to 1%). If the existing minimal cutsets are sufficient, then the increased risk level R_1 can be determined by setting the component-down unavailability to 1 and deleting larger minimal cutsets that contain smaller minimal cutsets (i.e., are absorbed by the smaller minimal cutsets). If there are any minimal cutsets containing complementary events, they also need to be removed if they are inconsistent with the component being down. The reduced risk level R_0 can be determined analogously by setting the down unavailability to zero.

If the component-down event is not contained in the existing minimal cutsets, or if there is a question on the coverage of the existing minimal cutsets, the minimal cutsets will then need to be regenerated. R_1 is determined by setting the down-component event in the PRA models to a true state. The truncation limit of the minimal cutset can be reduced by at least a factor of 10 to give added assurance of sufficient coverage. The minimal cutsets which are generated subsequently can then be used to determine R_0 by setting the down unavailability at zero.

Contributions from CCFs need special attention when calculating the increased risk level R_1 . If the component is down because of a failure, the common-cause contributions involving the component need to be divided by the probability of the component being down due to failure since the component is given to be down. If the component is down because it is being brought down for maintenance, the CCF contributions involving the component then need to be modified to remove the component and to only include failures of the remaining components (also see Section 4.3.1).

If other components are reconfigured while the component is down, these reconfigurations can then be incorporated in estimating R_1 or ΔR , using the PRA. If other components are tested before repair or if maintenance is carried out on the downed components, the conduct of these tests and their outcomes also can be modeled. If other components are more frequently tested when the component is down for the AOT, this increased frequency of testing also can be incorporated. These modeling details are sometimes neglected in the PRA because of their apparently small contribution. However, when isolating the AOT risk contributions and in justifying modified AOTs, these details can become significant.

Use of PRA Minimal Cutsets When It Is Appropriate

As indicated, a PRA computes the yearly AOT risk contribution to the yearly core-damage frequency (CDF). Basically, the yearly AOT risk contribution is the sum of the minimal cutset contributions containing the component-downed unavailability (typically, for maintenance) q_m ,

$$q_m = f \cdot d$$

where f is the downtime frequency and d is the downtime associated with the AOT. The downtime d usually is estimated as an average downtime associated with the AOT. If the minimal cutsets sufficiently cover the downed unavailability, those which contain the downed unavailability q_m can be summed to give the yearly AOT risk contribution R_y .

Using the PRA To Determine the Test-Limited Risk Contribution

The PRA can be used to calculate the increase in the risk level ΔR and to obtain the component unavailability, q , the contributing factors in calculating the test-limited risk contribution. The considerations involved in calculating R_1 and R_0 to obtain ΔR are those discussed above and in the next section.

DRAFT FOR COMMENT

When the effect of change in STI for one or more components is being evaluated, the PRA can be directly used to calculate the change in the risk measure, (e.g., in the CDF). The calculation of PRA results where changed STIs are included incorporates interactions among the STIs. The differences between the results (i.e., CDF when the STIs are changed from the baseline CDF) provides the test-limited risk contribution for changing the STIs.

In such a calculation, the contributions of CCFs need to be appropriately modified. The common failure terms modeled as a function of the test interval should be modified to reflect the new STI. Typically, CCFs are modeled using a β -factor or Multiple Greek Letter model where the CCF of multiple components is a function of the STI. When changing STIs, care should be taken to change this term within the common-cause contribution. The common cause of failing multiple components resulting from human error following a test is not a function of the STI, but may be affected by the test strategy used.

When different test strategies are being evaluated, the human error term needs to be evaluated. Specific assumptions that were used in quantifying the human error common-cause term should be identified and checked if they apply for the test strategy being analyzed. For example, if the term was developed assuming a sequential test strategy, but a staggered test strategy is being analyzed, the term then needs to be modified to reflect this change. The failure probability from a common-cause human error for a staggered test strategy is expected to be significantly lower than that for the sequential test strategy.

Using Minimal Cutsets To Calculate Test-Limited Risks

The test-limited risk for a component or a set of components also can be determined by identifying those minimal cutsets which contain one or more of the STI contributions. The sum of the relevant minimal cutset contributions is then equal to the test-limited risk. To evaluate changes in the test-limited risks for changes in the STIs, the difference between the minimal cutset contributions with and without the STI changes will be the difference between the test-limited risks. In using the minimal cutsets, one should ensure that the STI contributions are all included in the set of minimal cutsets used. Even though use of the minimal cutsets gives the same results, the above basic formulas for the test-limited risks are useful, since they show the basic contributing factors to the STI risk.

Specific Considerations for Evaluating Multiple Test-Limited Risks

When multiple STIs are modified or are defined, the total test-limited risk from the multiple STI changes or definitions needs to be properly evaluated. Instead of using the PRA to evaluate all the modifications in a given run, the individual test-limited risks can be evaluated one at a time, provided that the updated STIs are used for the other relevant components. An iterative procedure can then be used in which individual STIs are successively updated, using the formulas given above for individual component STI risk contributors. These one-at-a-time evaluations, or "iterative" evaluations, are useful if acceptable guidelines on test-limited risks are defined, and the STIs are to be selected to satisfy the risk guidelines.

A.1.3.2 Appropriate Calculation of Conditional CDF

Conditional CDF for Failure of a Component

To calculate the conditional CDF when a component is failed (typically represented by R_1 in this document), the component unavailability is changed to the "true" or "T" state. However, the component unavailability may be modeled in terms of many contributors: random failure, maintenance downtime, test downtime, and CCF. The CCF term represents the failure probability of two or more redundant components which include the failed component in question. The CCF term is modeled as a product of multiple terms (e.g., using the β -factor model for two redundant components, the CCF term is β times the component unavailability from random failures), but may be represented by one parameter.

Consider a component Q in Train A of a safety system, letting Q_{LA} , Q_{MA} , and Q_{TA} represent the component's unavailability from random failures, maintenance downtimes, and test-downtimes, respectively. Also, let $QC(=\beta \cdot QL)$ be the term for CCF of the redundant components in Trains A and B, where QL is numerically equal to Q_{LA} and represents Q_{LA} or Q_{LB} . Q_{LB} is the unavailability of a component in Train B from random failure. Usually, the terms Q_{LA} , Q_{MA} , Q_{TA} , and QC will be part of the PRA input data.

To calculate the conditional CDF given that the component is failed, the component unavailability should be represented by the "T" state. This means that Q_{LA} , Q_{MA} , and Q_{TA} should be changed to the "T" state and QC should be divided by Q_{LA} since the component is down because of failure. In principle, changing one of the three conditions (Q_{LA} , Q_{MA} , Q_{TA}) to the "T" state should suffice. However, in many cases, truncated cutsets are used to calculate the conditional CDF, and changing all three will ensure that the failed state of the component is represented. For this example, QC will be changed to β , which represents the conditional failure probability of the redundant component. When QC represents the failure of more than two components, QC will be converted to the failure probability of the remaining components, in this case, two components.

Conditional CDF When a Component Is Down (but Not Failed) for PM

To calculate the conditional CDF when a component is taken down for PM (R_1 for PM analyses), the CCF term needs to be treated differently from that described above for the failure of the component.

Considering the same example as above, the down state of the component is represented by changing Q_{LA} , Q_{MA} , and Q_{TA} to "T" and by changing QC to QL , which is numerically the same as Q_{LB} or Q_{LA} . The CCF term is changed to represent the unavailability of the remaining component and not β , since the initial component is already down for PM and is not down due to failure. If the redundant component is successfully tested before taking the component down for PM, QC can then be equated to zero for a short-duration PM (i.e., when the duration of the PM is much less than the test interval).

DRAFT FOR COMMENT

Conditional CDF When the Component Is Not Down for Maintenance or Is Tested Operable

The conditional CDF is reduced when the component is not down for maintenance or when it has just successfully been tested. The calculation of AOT and STI risk contributions involve calculating this conditional CDF (R_o). For evaluating the AOT risk contribution, R_o signifies that the component is not down for test or maintenance, and this condition is represented by setting test and maintenance downtime unavailabilities to the "false" or "F" state. In this example, QMA and QTA should be changed to the "F" state. For STI evaluations, R_o signifies that the component is up, which is known from the test and is represented by setting its unavailability to "false." In this example, QLA, QMA, and QTA should be changed to the "F" state. In many cases, the reduction in CDF from the baseline CDF is negligible.

Conditional CDF When Multiple Components Are Involved

To calculate conditional CDFs (R_1 and R_o) when multiple components are involved, the corresponding terms relating to each of the components should be changed to the "T" or "F" state. For each component, the corresponding terms relating to random failures, CCFs, test downtimes, and maintenance downtimes should be converted, as discussed above. When all the components modeled by a common-cause term are failed, this term changes to the "T" state for calculating R_1 . Otherwise, it is modeled as discussed above, representing the unavailability of the remaining components. In many PRA computer codes, the CCF term does not retain the specific component designator (for example, a unique notation identifying the specific component involved may not be part of the name of the CCF term), and the relevant term cannot directly be identified by searching the names of the input parameters of the PRA. The description of the CCF terms modeled in the PRA may need to be examined to identify the relevant term or the input parameter.

A.1.3.3 Treatment of CCF and Recovery Factors

The treatment of CCF in estimating the conditional CDF for AOT and STI evaluations was discussed earlier. Appropriate considerations in modifying CCF terms modeled in the PRA (to include the effect of a component being unavailable because of failure, maintenance, or testing and for implementing a staggered test strategy) have been discussed. In addition, since the CCF contributions can be a dominant contributor, sensitivity analyses with respect to these parameters are suggested in Section 4.5. Recovery factors used in the PRA model may need to be reviewed to learn if the component assumed to be down because of failure is credited to be recovered. For example, consider that a TS change for an emergency diesel generator (EDG) is being evaluated, and conditional CDF for the EDG being down is being calculated. Then, if the cutsets used to calculate the conditional CDF take credit for the same EDG being recovered, such recovery factors should be modified. In such cases, no credit should be taken.

A.1.3.4 Calculations of Transition Risk

Transition risk is calculated to compare the risk of continuing operation in a given LCO to that of a transition to plant shutdown. Such comparisons can be used to decide which option is preferable and which other alternatives may be used. Such evaluations particularly apply for systems used to remove decay heat. The following considerations apply in calculating transition risk:

- (1) Various stages of the shutdown cooling phases and the operator's interactions, should be modeled to assess the impact on the CDF of shutting down the plant in a LCO.
- (2) Any initiating event not modeled in the basic PRA, but important during the shutdown phases, should be modeled. Specific examples are those events that challenge the residual heat removal (RHR) system and that can render part of it unavailable. Also, the frequency of initiating events during the transition to shutdown may have to be reassessed, since it may differ from that during power operation (e.g., more frequent loss of offsite power or loss of main feedwater during the transition to shutdown).
- (3) Different recovery paths applicable at various stages of shutdown should be modeled to realistically quantify the risk of shutting down, considering the diminishing levels of decay heat.
- (4) Available time margins for uncovering the reactor core and heating up the suppression pool [in a boiling water reactor (BWR)] or drying out the steam generator [in a PWR] need to be modeled to evaluate specific accident sequences.

A.2 Data Needs for TS Change Evaluations

A request for plant-specific TS changes should use plant-specific data and not rely solely on generic data or data from similar plant designs. Usually, TS changes are requested because plant operation indicates that such changes are needed and accordingly, plant-specific data are expected to be available. For the components or systems for which TS changes are being considered, plant-specific data should be evaluated and assurance should be obtained that the data used are consistent with the plant experience. The use of other than plant-specific data should be justified.

When a generic analysis is being performed using a representative plant model, the use of generic data from similar plants is acceptable. The generic data should bound the specific plants under consideration, not an average plant.

A.2.1 Care in Using Plant-Specific Data

When plant-specific data are used to update input parameters of the PRA during a TS change evaluation (additional to that used during the latest update of the PRA), care should be taken that such data are consistently used both for the base case, where existing TS requirements apply, and the change case,

where TS changes are incorporated. This is done to ensure that the increase in the risk measure obtained is due to the TS change only and not to the use of plant-specific data in aspects of plant operation.

This situation typically arises when recent plant-specific data are evaluated and reduced values of the parameters are obtained. Use of the reduced values may negate the risk increase from the TS change and may give an erroneous impression that the TS change has reduced the risk. When the base case is also updated, such difficulties are avoided. Sensitivity and uncertainty analyses should also be performed using the same set of input data.

A.2.2 Considerations When Generic Data Are Used

When generic data are used for the TS parameters in evaluating TS changes, focus should be on justifying very small changes which do not strongly depend on the data parameters. Reasons why generic data are being used and why generic data apply for plant-specific evaluations should be presented. In many cases, because of limited experience, use of plant-specific data may result in very optimistic values justifying use of generic data.

A.2.3 Specific Data Needs

Basic data needed for a PRA-informed TS change evaluation for risk-informed regulation are those collected as part of the PRA. Comparative risk calculations for LCO changes require no additional data beyond those in the Full-power Operations Level 1 and the Low Power/Shutdown Level 1 PRAs. The additional data needs for evaluating changes in surveillance requirements [such as surveillance test intervals (STI)] and allowable outage times (AOT) are discussed in this subsection.

A.2.3.1 Maintenance-Downtime Data

The maintenance downtime data require partitioning it into plant-specific unplanned unavailability for unscheduled maintenance and planned unavailability for preventive maintenance or testing. For this purpose, data are needed on the frequency of events leading to planned and unplanned maintenance, i.e., the number of occurrences of each type of downtime event during a given time period, and the time interval that the component was out of service for each occurrence. These data are also needed for judging whether an adequate AOT is being provided to complete a repair. The distribution of downtimes also can be used to estimate the expected risk for a given AOT.

The distribution of time for unscheduled maintenance may shift when an AOT is being changed. For this reason, information about such an influence on the distribution is not expected to be available when the AOT modification is being evaluated. The average downtime can be assumed to proportionally increase with the increase in the proposed AOT for downtimes associated with unscheduled maintenance. For scheduled (preventive) maintenance, the downtime assumed can be representative of plant practices (e.g., one-half of the AOT).

A.2.3.2 Maintenance Schedules and Frequency

These data include the maintenance scheduling used by the plant for defining the situations in which multiple equipment or system trains may be taken down for PM. These schedules are important to ensure that high risks from components being simultaneously down, implicitly allowed by the TS change, do not occur.

The maintenance frequency or frequency of downtime for a component may be from 3 to 10 times higher than the failure frequency. Since AOTs can be used for maintenance, the frequency of maintenance should be incorporated in estimating the downtime frequency.

A.2.3.3 Data Relating to Component Testing

The following data related to component testing, in addition to those available as part of the PRA study, form part of a TS change evaluation relating to surveillance requirements:

- a list of the components being tested, any component realigned from the safety position during a test, duration of the test, and the test frequency recommended by the manufacturer
- the efficiency of the test (i.e., the failure modes detected by the test in regard to components, support system interfaces, and so forth). Bounding assumptions can be made if obtaining detailed data or related information is costly.
- Any potential for negative effects of surveillance testing (e.g., that may cause the potential for introducing plant transients, or that may cause unnecessary wear of the equipment) should be taken into account by the analyses. Preliminary evaluations can be used to determine if a more detailed analysis should be performed.
- The test strategy used for the redundant components in a system (i.e., whether staggered or sequential testing is performed) should be stated. The standard PRA quantification assumes that components follow no specific schedule and are randomly placed with regard to one another. By staggering the test times of components in different trains, the test-limited risk contribution will be reduced for the same STIs as compared to the PRA assumption. Conversely, if the tests are carried out sequentially, the test-limited risk will increase compared to the PRA assumptions.

A.2.3.4 Parameters for Component Unavailability

The component unavailabilities used in a PRA contain a number of parameters that are relevant for evaluating TS changes. These parameters should be delineated, as modeled, to facilitate evaluations to be conducted and reviewed by the regulatory authority. The following desirable parameters contributed to the estimated component unavailability:

- component failure rate
- component test interval
- maintenance/repair downtime contribution (maintenance frequency, downtime for scheduled and unscheduled maintenance)
- test downtime, if applicable
- human errors following test or maintenance, if modeled
- separation of cyclic-demand vs. standby time contribution, if modeled

A.2.3.5 Separating Demand and Standby Time Contributions to Unavailability

Since the test-limited risk (typically defined as R_D) is associated with a failure occurring between tests, the failure rate that should be used in calculating the test-limited risk should be the standby time-related failure rate, which is associated with what can occur while the component is in standby between tests. Test-limited risk contributes to increases in risk associated with longer test intervals due to the longer time to detect standby-stress failures. The time-related failure rate is expressed in units per time period, such as per hour. For estimating R_D , the data needed are the standby stress failure rate of the component and the proposed test interval.

The failure probability of a component consists of a time-related contribution (the standby time-related failure rate), and a cyclic, demand-related contribution (the demand stress failure probability). The latter is the probability contribution associated with failures which are caused by demanding, starting, or cycling the component, which include (but are not necessarily limited to) test-caused transients as discussed below in subsection 5.4.3.6. Since the test-limited risk, R_D , is associated with a failure occurring between tests, the failure rate that should be used in calculating the test-limited risk is the time-related standby stress failure rate. From the total number of failures on demand, the number of failures due to standby stress and the number of failures from demand stresses can be partitioned by either an engineering analysis of failure causes or by a graphical method based on the relationship between the observed number of failures and the test interval lengths from which the failures came.

The test caused contribution to risk is primarily composed of R_{down} , the risk contribution due to the unavailability of equipment resulting from aligning equipment away from its preferred position/state to conduct a test, when there is no automatic return to the preferred position. The additional data needed for estimating this parameter are the surveillance test interval and the out-of-service time needed for each test.

Dividing the failure probability into a time related and cyclic demand-related contribution results in a lower test-limited risk because only part of the component's failure rate is treated as time related. However, treating only part of the failure rate as being time related when this is not the case underestimates the test limited risk; therefore, such a breakdown of the failure rate needs to be justified through data analysis or engineering analyses.

Also, sometimes only the failure probability (i.e., the component unavailability q) may be provided without giving a failure rate. In such a case, the effect of a change in the test interval cannot be evaluated unless the component test interval previously used for true T is used to convert the unavailability q in terms of λ and T . When the breakdown between time-related and cyclic demand-related contribution is unknown, all failures can be assumed to be time related to obtain the maximum test-limited risk contribution.

In summary, the data required for measuring a change in risk with a change in the surveillance test interval are a breakdown of the failure probability of the component into its time-related and demand-related components, the proposed test interval, and the out-of-service time for surveillance testing for the component.

A.2.3.6 Test-Caused Transients

To evaluate and identify the test-caused transients risk (typically defined as R_C), transient events should be analyzed and those caused by a test should be identified. In most cases, this requires reading through the description of transients that have occurred and noting those caused by the test. When longer test intervals are allowed, the resulting reduction in test-caused transients per unit time tends to cause decreases in risk due to fewer adverse effects of testing over that longer test interval (which, however, will be partially or wholly balanced by increased in R_D that are caused by the longer time period before detection and correction of failures).

The transient events are obtained from the following plant operating data:

- (1) Performance indicator reports: These reports list the number of reactor trips and safety system actuations at each plant, the date of the events, and the numbers of the relevant licensee event reports (LERs).
- (2) LER system: Reactor trips are described in LERs.

When test-caused transients for a single plant are evaluated, the plant-specific data may be sparse unless the plant's operating experience covers a substantial period. When this is the case, more data may be used from the operating experience of other plants of similar vintage (for example, other BWR/4s) assuming that the likelihood of occurrence of test-caused transients is similar for all the plants in the data base. (The performance indicator reports categorize plants according to design classes.)

A.2.3.7 Data for Evaluating Transition Risk

Data available in a PRA for full-power operation provide the basic information for evaluating the transition risks when a plant is being shut down for an LCO. In addition, the PRA for low-power and shutdown operations, if available, will significantly ease the acquisition of the data necessary for evaluating the risk of shutdown. The low-power and shutdown PRAs typically contain relevant data, such as the durations of

DRAFT FOR COMMENT

shutdown phases and the frequencies of initiators that may occur during shutdown operation (e.g., loss of RHR).

The full-power PRA is available for most operating plants, but the low-power and shutdown PRAs may be available only for some plants. Hence, the data needed to evaluate transition risk are discussed here, assuming that only data from a full-power PRA are available:

- (1) Plant-specific data on shutdown operations: To analyze shutdown phases in detail, plant-specific information may be needed, such as operating and abnormal procedures, shift supervisor's log books, or monthly operating reports. From this information, data on timing of the plant shutdown and operational preferences of equipment during plant shutdown can be extracted.
- (2) Plant-specific traditional data: The evaluation of heatup and recovery scenarios, including estimates of heatup time, requires some design data on the plant, such as the temperature of the ultimate heat sink, or the cooling capacity of the RHR system. These data typically are available from the plant's final safety analysis report (FSAR).
- (3) Frequency of transients during controlled shutdown: The LERs for the plant may need to be reviewed in order to evaluate the likelihood of transients during controlled shutdown. The likelihood of a transient during a shutdown may be different from that during power operation (this should be considered).



UNITED STATES NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

DRAFT FOR COMMENT

**Use of Probabilistic Risk Assessment in
Plant-Specific, Risk-Informed Decisionmaking:
General Guidance**

Draft SRP Chapter 19

Revision L

March 27, 1997

Contacts: M. P. Rubin (301) 415-3234
M. C. Cheok (301) 415-8380

STANDARD REVIEW PLAN

USE OF PROBABILISTIC RISK ASSESSMENT IN PLANT-SPECIFIC, RISK-INFORMED DECISIONMAKING: GENERAL GUIDANCE

TABLE OF CONTENTS

| | |
|--|----|
| <u>INTRODUCTION</u> | 1 |
| <u>ROLES AND RESPONSIBILITIES</u> | 2 |
| I. <u>AREAS OF REVIEW</u> | 3 |
| II. <u>REVIEW GUIDANCE AND PROCEDURES</u> | 5 |
| II.1 <u>General</u> | 5 |
| II.2 <u>Element 1: Define the Proposed Change</u> | 6 |
| II.3 <u>Element 2: Conduct Engineering Evaluations</u> | 7 |
| II.3.1 <u>Evaluation of Defense-in-Depth Attributes and Safety Margins</u> | 7 |
| II.3.1.1 <u>Defense-in-Depth</u> | 7 |
| II.3.1.2 <u>Safety Margins</u> | 10 |
| II.3.1.3 <u>Current Regulations</u> | 11 |
| II.3.2 <u>Risk Assessment</u> | 12 |
| II.3.2.1 <u>Characterization of Change in Terms of PRA Model Elements</u> | 13 |
| II.3.2.2 <u>Scope of Analysis</u> | 13 |
| II.3.2.3 <u>Level of Detail</u> | 14 |
| II.3.2.4 <u>Quality of a PRA for Use in Risk-Informed Regulation</u> | 15 |
| II.3.2.5 <u>Risk Impact Including Treatment of Uncertainty</u> | 17 |
| II.3.3 <u>Integrated Decisionmaking Process</u> | 22 |
| II.4 <u>Element 3: Develop Implementation and Monitoring Strategies</u> | 22 |

DRAFT FOR COMMENT

| | | |
|------------|--|------|
| II.5 | <u>Element 4: Staff Evaluation of Submittal</u> | 24 |
| III. | <u>EVALUATION FINDINGS</u> | 29 |
| IV. | <u>IMPLEMENTATION</u> | 34 |
| V. | <u>REFERENCES</u> | 35 |
| Appendix A | GUIDANCE FOR A FOCUSED-SCOPE APPLICATION SPECIFIC PRA REVIEW | A-1 |
| A.1 | <u>Use of Appropriate Data</u> | A-1 |
| A.2 | <u>Initiating Events</u> | A-4 |
| A.3 | <u>Determination of Success Criteria</u> | A-6 |
| A.4 | <u>Modeling of Common Cause Failures</u> | A-7 |
| A.5 | <u>Modeling of Human Performance</u> | A-9 |
| A.6 | <u>Effects of Truncation Limits Used</u> | A-12 |
| Appendix B | INTEGRATED DECISIONMAKING | B-1 |
| Appendix C | CATEGORIZATION OF STRUCTURES, SYSTEMS, AND COMPONENTS WITH RESPECT TO SAFETY SIGNIFICANCE | C-1 |
| C.1 | <u>Use of Importance Measures</u> | C-2 |
| C.2 | <u>Role of Integrated Decisionmaking in Component Categorization</u> | C-5 |

STANDARD REVIEW PLAN

USE OF PROBABILISTIC RISK ASSESSMENT IN PLANT-SPECIFIC, RISK-INFORMED DECISIONMAKING: GENERAL GUIDANCE

19.0 USE OF PRA IN REGULATORY ACTIVITIES: 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 licensee proposals for changes to a plant's current licensing basis (CLB)¹. The SRP identifies the types of information that may be used in each activity and provides general guidance on how the information from a probabilistic risk assessment (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 commission's PRA policy statement and PRA implementation plan (references 1, 2 and 3). In developing this document, the staff has considered the NRC regulatory guide on the use of PRA in risk-informed regulatory applications, draft Regulatory Guide DG-1061 (Reference 5) and the relevant industry guidance documented in Reference 4. In addition, reference will be made to other SRP chapters which provide additional guidance for the review of specific applications of PRA in regulated activities.

Risk-informed decisionmaking will be based on the following approach. The design, construction, and operational practices of the plant being analyzed are expected to be consistent with its CLB. The risk evaluations performed to justify regulatory changes are expected to realistically reflect the plant-specific design, construction, and operational practices. The PRA analyses should be as realistic as practicable, and should address significant uncertainties. Results of these risk analyses will be part of the input to the decision process that evaluates margin in plant capability (both in performance and in redundancy/diversity). The decision process will use the

¹ This SRP adopts the 10 CFR Part 54 definition of current licensing basis, i.e., "CLB is the set of NRC requirements applicable to a specific plant and a licensee's written commitments for ensuring compliance with and operation within applicable NRC requirements and the plant-specific design basis (including all modifications and additions to such commitments over the life of the license) that are docketed and in effect. The CLB includes the NRC regulations contained in 10 CFR Parts 2, 19, 20, 21, 26, 30, 40, 51, 54, 55, 70, 72, 73, 100 and appendices thereto; orders; license conditions; exemptions; and technical specifications. It also includes the plant specific design-basis information defined in 10 CFR 50.2 as documented in the most recent final safety analysis report (FSAR) as required by 10 CFR 50.71 and the licensee's commitments remaining in effect that were made in docketed licensing correspondence such as licensee responses to NRC bulletins, generic letters, and enforcement actions, as well as licensee commitments documented in NRC safety evaluations or licensee event reports."

DRAFT FOR COMMENT

risk results in a manner which complements traditional engineering approaches and supports the defense-in-depth philosophy and preserves safety margins. 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 the Office of Nuclear Reactor Regulation (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 appropriate regulatory document, and coordinating any input 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), at the request of the primary review branch, is responsible for review of the PRA information and findings submitted by the licensee. Review support includes the assessment of the adequacy of the scope, level of detail and quality of the PRA used by the licensee to support the regulatory change and the application of risk related acceptance guidelines to support decisionmaking.

The Reactor Systems Branch (SRXB), at the request of the primary review branch or SPSB, provides support in accident sequence modeling, including treatment of reactivity and thermal-hydraulic phenomena, system response, and the implementation of emergency operating procedures and abnormal operating procedures.

The Containment and Severe Accident Branch (SCSB), has primary responsibility for review of any containment response and containment integrity information submitted by the licensee in support of a request for regulatory action.

The Emergency Preparedness and Radiation Protection Branch (PERB) has primary responsibility for review of any evaluations of radionuclide contamination or public health effects submitted by a licensee in support of a request for regulatory action.

The Office of Nuclear Regulatory Research (RES), at the request of the primary review branch, provides technical support in areas involving all aspects of PRA, severe accident phenomenology and engineering studies.

The Office for Analysis and Evaluation of Operational Data (AEOD), at the request of the primary review branch, provides generic and plant-specific data on the frequency of initiating events, common cause failures and human errors from operating experience.

The Regional Offices, at the request of the primary review branch, provides information on licensee operational experience in areas of system performance, operator performance, risk management practices and management controls.

DRAFT FOR COMMENT

I. AREAS OF REVIEW

The NRC's PRA Implementation 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 licensing amendment requests submitted for NRC review and approval for which PRA can play an effective role in the decisionmaking process. General review guidance for applicable activities is presented in this SRP. In addition, application-specific SRP chapters are available to provide additional guidance for several activities. Examples 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 pumps and valves in a licensee's inservice test (IST) program;
- Changes in scope and frequency of inspections in a licensee's inservice inspection (ISI) program; and
- Grading of activities in the licensee's quality assurance (QA) program.

Draft regulatory guide DG-1061 defines an acceptable approach to analyzing and evaluating proposed CLB changes. This approach supports the staff's desire to base its decisions on the results of traditional engineering evaluations, supported by insights (derived from the use of PRA methods) on the risk significance of the proposed changes. The decision process leading to the proposed change is expected to be done in an integrated fashion (considering traditional engineering and risk information) and may be based upon qualitative factors as well as quantitative analyses and information.

As discussed later in this section, the scope of the staff review of a risk-informed application will depend on the specifics of the application. However, this scope should include a review of the four-element approach as suggested in chapter 2 of draft Reg Guide DG-1061. The areas of review for each of these elements are summarized below.

Element 1: Define the Proposed Change

The objective of this element is to provide the groundwork for the evaluation of safety impacts of the proposed change. Areas of review in this element therefore includes an evaluation of: the proposed change in light of the CLB; the structures, systems and components (SSCs), procedures and activities that are covered by the proposed change; the method of analysis; and the available engineering studies and risk evaluation findings that are relevant to the proposed change.

Element 2: Conduct Engineering Evaluations

In this element, the reviewer should evaluate the proposed change to ensure that defense-in-depth and safety margins are maintained, and that the calculated change in plant risk is within the guidelines specified in DG-1061. The proposed changes are to be evaluated in light of the licensee's risk management approach in which the licensee is using risk analysis to improve operational and engineering decisions and not just to eliminate requirements the licensee sees as undesirable, and that cumulative risk impacts are appropriately factored into the decision process.

Element 3: Develop Implementation and Monitoring Strategies

Implementation and monitoring strategies can provide early indication of plant performance under the proposed changes and these strategies are therefore important in applications where there is some uncertainty in evaluation models and/or data. As such, the review scope should include provisions to ensure that the licensee proposed process for implementation and monitoring is adequate to in part account for uncertainties with regard to plant performance under the proposed change.

Element 4: Document Evaluations and Submit Request

The reviewer should assure that the submittal includes sufficient information to support conclusions regarding the acceptability of the proposed change and that archival documentation of the evaluation process and findings is maintained and available for staff audit and review. The reviewer should also assure that the appropriate regulatory action is requested, for example, a license amendment, an exemption, or a change to technical specifications. Where appropriate, these actions should include enhancements in regulatory requirements to preserve the assumptions in the supporting risk analysis, and to assure that high risk significant SSCs not currently subject to regulatory control will be subject to requirements commensurate with their risk significance. Finally, the reviewer should assure that CLB changes are appropriately included in a Safety Analysis Report update as necessary.

Application-Specific Reviews

This SRP chapter is written to provide guidance for a full scope review of applications in risk-informed regulation where evaluation findings are dependent on the numerical values of risk indices and where a broad set of scenarios and plant operating modes may be affected. Where it is determined that an application could justify a review that is less than full scope, the reviewer should choose the relevant and applicable parts of this SRP for guidance. In addition, some applications may be supportable without resort to the level of integration and quantitative perspective afforded by PRA, and correspondingly, little or no staff review of the PRA may be necessary. Application-specific SRP chapters (where available) will provide additional guidance in this area.

II. REVIEW GUIDANCE AND PROCEDURES

II.1 General

For each risk-informed application, reviewers should ensure that the following principles for risk-informed decisionmaking are met (SRP sections dealing with each principle are provided in parenthesis):

- The proposed change meets the current regulations. This principle applies unless the proposed change is explicitly related to a requested exemption or rule change (i.e., a 50.12 "specific exemption" or a 2.802 "petition for rulemaking") (section II.3.1);
- Defense-in-depth is maintained (section II.3.1);
- Sufficient safety margins are maintained (section II.3.1);
- Proposed increases in risk and their cumulative effect are small, and these changes do not cause the NRC Safety Goals to be exceeded (sections II.3.2 and II.3.3); and
- Performance-based implementation and monitoring strategies are proposed that address uncertainties in analysis models and data, and provide for timely feedback and corrective action (section II.4).

In demonstrating the above, reviewers should ensure that the following have been addressed as part of the submittal:

- All safety impacts of the proposed change are evaluated in an integrated manner as part of an overall risk management approach in which the licensee is using risk analysis to improve operational and engineering decisions broadly and not just to eliminate requirements the licensee sees as desirable. The approach used to identify changes in requirements was used to identify areas where requirements should be increased as well as where they could be reduced (section II.3.3);
- The acceptability of the proposed changes is evaluated in an integrated fashion that ensures that all principles are met (section II.3.3);
- Increases in estimated CDF and LERF resulting from proposed CLB changes are limited to small increments (section II.3.2);
- The scope and quality of the engineering analyses (including traditional and probabilistic analyses) conducted to justify the proposed CLB change are appropriate for the nature and scope of the change and are based on the as-built and as-operated and maintained plant (section II.3.2);
- Appropriate consideration of uncertainty is given in analyses and

DRAFT FOR COMMENT

interpretation of findings (section II.3.2);

- The plant-specific PRA that is used to support licensee proposals has been subjected to quality controls such as an independent peer review (section II.3.2); and
- Data, methods, and assessment criteria used to support regulatory decisionmaking are available for public review (section II.5).

II.2 Element 1: Define the Proposed Change

In this element, the reviewer should verify that enough information is provided to meet the staff's expectation that all potential safety impacts have been identified and evaluated. In addition, the reviewer should be satisfied that, where appropriate, the licensee has identified design and operational aspects of the plant related to the change request that should be enhanced consistent with an improved understanding of their safety significance based on the methodology use to support the proposed relaxation in regulation. These enhancements should be appropriately-reflectd in licensing basis changes (e.g., technical specification, license conditions, and FSAR)

The proposed changes should be reviewed with regard to the current licensing basis. The licensing basis of the plant documents how the licensee satisfies certain basic regulatory requirements such as diversity, redundancy, defense-in-depth, and the General Design Criteria.

Engineering (or other pertinent) analysis and data that identify the safety margins or plant activities conducted to preserve those margins should be reviewed. If exemptions from regulations or relief requests are needed to implement the licensee's proposed change, the reviewer should ensure that the appropriate requests accompany the licensee's submittal.

The reviewer should verify that available documents reflecting traditional engineering concepts and principles have been identified and appropriately used. 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, and the bases for Technical Specifications such as Limiting Conditions for Operation (LCOs), Allowed Outage Times (AOTs), and Surveillance Requirements (SRs).

Where available, plant specific data and operational information should be factored into the evaluation process. Reviewers should consider the way in which the issues at hand are reflected in operational data. 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

DRAFT FOR COMMENT

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.

Finally, as part of the initial review of the licensing amendment, the reviewer should determine if the scope of the impact of the proposed change has been adequately characterized (specifically, if all SSCs affected by the proposed change have been identified) and if the analysis performed and submitted have the scope and depth needed to adequately characterize the impact of this change.

II.3 Element 2: Conduct Engineering Evaluations

In order for the staff to make findings of acceptability regarding a proposed license amendment, the staff position should be based on an integrated assessment of traditional engineering evaluations and probabilistic information. Specific evaluations expected to be performed by the licensee are described in section 2.4 of draft reg guide DG-1061. The scope and quality of the engineering analyses conducted to justify the proposed change should be appropriate for the nature and scope of the change. Types of traditional engineering and probabilistic information which should be included in submittals are described in section 3 of the draft guide.

The results of this element should be reviewed to determine if the following principles for risk-informed decisionmaking are satisfied: the proposed change meets current regulations unless the change is explicitly related to a requested exemption or rule change; defense-in-depth is maintained; sufficient safety margins are maintained; and proposed increases in risk and their cumulative effect are small, and these changes do not cause the NRC Safety Goals to be exceeded.

II.3.1 Evaluation of Defense-in-Depth Attributes and Safety Margins

A review of the engineering evaluations should be performed to demonstrate that the principles identified in Section II.1 are not compromised. These evaluations should include not only the traditional design basis accident (DBA) analyses, but also evaluations of the defense-in-depth attributes of the plant, safety margins, and risk assessments performed to obtain risk insights and quantification of the impact of the proposed change.

II.3.1.1 Defense-in-Depth

Defense-in-depth is defined as a philosophy which ensures that successive measures are incorporated into the design and operating practices for nuclear plants to compensate for potential failures in protection and safety measures.

DRAFT FOR COMMENT

In risk informed regulation, the intent is to assure that the philosophy of defense-in-depth is maintained, not to prevent changes in the way defense-in-depth is achieved. The defense-in-depth philosophy has been and continues to be an effective way to account for uncertainties in equipment and human performance. In some cases, risk analysis can help quantify the range of uncertainty; however, there will likely remain areas of large uncertainty or areas not covered by the risk analysis. Where a comprehensive risk analysis can be performed, it can be used to help determine the approximate extent of defense-in-depth (e.g., balance among core damage prevention, containment failure and consequence mitigation) to ensure protection of public health and safety. However, because all aspects of defense-in-depth are not reflected in PRAs, appropriate traditional defense-in-depth considerations should also be used to account for uncertainties.

Preservation of Multiple Barriers for Radioactivity Release

Defense-in-depth can be argued based on considerations of the barriers that prevent or mitigate radioactivity release. Release of radioactive materials from the reactor to the environment is prevented by a succession of 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 for accident consequence mitigation. 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 to support the functional performance of each barrier.

In maintaining the defense-in-depth philosophy, the proposed license amendment should not result in any substantial change in the effectiveness of barriers. The following are review objectives to ensure that the proposed change maintains appropriate safety within the defense-in-depth philosophy:

- the change does not result in a significant increase in the existing challenges to the integrity of the barriers;
- probability of failure of each barrier is not significantly changed by the proposal;
- new or additional failure dependencies are not introduced among barriers that result in a significant increase in the likelihood of failure compared to the existing conditions; and
- the overall redundancy and diversity in the barriers is sufficient to be compatible with the risk acceptance guidelines.

In demonstrating the above, it is a staff expectation that, for the proposed change:

- a reasonable balance among prevention of core damage, prevention of

DRAFT FOR COMMENT

containment failure, and consequence mitigation is preserved;

- over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided;
- system redundancy, independence, and diversity are preserved, commensurate with the expected frequency and consequences of challenges to the system;
- defenses against potential common cause failures are preserved and the introduction of new common cause failure mechanisms is assessed;
- independence of barriers is not degraded; and
- defenses against human errors are preserved.

The above elements can be addressed by using qualitative or traditional engineering arguments or by using PRA results contained in the model sequences and cutsets.

Role of PRA in Review of Defense-in-Depth

In addition to the usual quantitative risk indices, PRAs provide important qualitative results, namely, the accident sequence minimal cutsets. Each accident sequence minimal cutset is a combination of passive and active SSC failures and human errors that would cause core damage or a radioactivity release. The cutsets therefore directly show one particular aspect of defense-in-depth, in that they reveal how many failures must occur in order for core damage or a radiological release to occur. The minimal cutsets therefore show the effective redundancy and diversity of the plant design.

Events appearing in each minimal cutset are, in most cases, targeted by programmatic activities to assure the reliability of the associated SSC. Specific activities that are important in maintaining reliability of a component include: inservice testing, inservice inspection, periodic surveillance required by Technical Specifications, quality assurance, and maintenance. Therefore, when a review of the minimal cutsets shows areas where redundancy or diversity are already marginal, it would arguably be inappropriate to reduce the level of activities aimed at ensuring SSC performance, unless the activities can be shown to have little or no effect on SSC performance or if it can be shown that uncertainties in the performance of the elements in this cutset are well understood and quantified. It is also possible that compensating or alternative activities could be proposed to provide assurance of SSC performance. The objective of this review is to avoid completely relaxing the defense-in-depth posture at points at which the plant design has the least overall functional independence, redundancy, and/or diversity. On the other hand, in areas where a plant has substantial redundancy and diversity, defense-in-depth arguments used to justify relaxations should be given appropriate weight.

DRAFT FOR COMMENT

As part of the review of defense-in-depth, the effects of multiple component failures that could potentially result from the proposed change should be evaluated. For example, if all events in a cutset have been proposed for a reduction in requirements, the reviewer should ensure that the effect of the change is modeled properly and that the change does not have an adverse effect on defense-in-depth.

Finally, in the review of sequence cutsets, attention should be given to potential over-reliance on programmatic activities or operator actions that compensate for weaknesses in the plant design. For example, proposed maintenance and surveillance activities should complement and not replace proper plant design.

II.3.1.2 Safety Margins

In the determination of the design performance characteristics of a system, safety margin represents an allowance for uncertainty in SSC performance. Current safety analysis practices incorporate consideration of margin in most areas. As examples, many engineering standards, licensing-analyses, and technical specifications take margin into account.

Incorporating margin can result in over-designing of components, incorporation of extra system trains or extra systems, or in conservative operating requirements for systems and components. Therefore, some licensee applications will seek to reduce this margin in some areas. Reduction of margin should appropriately reflect the current understanding of existing uncertainties and the potential impact of the proposed change.

Therefore, as part of the review of the impacts of a proposed change, its effects on safety margins should be evaluated. For example, the reviewer should establish that:

- engineering codes and standards or alternatives approved for use by the NRC are met, or deviations are justified; and
- safety analysis acceptance criteria in the current licensing basis are met, or proposed revisions provide sufficient margin to account for analysis and data uncertainty.

Clearly, these items are closely related to guidance provided in section II.3.1.3 regarding the need to maintain the current CLB. The thrust of the guidance in the present section is to sensitize reviewers to the implications of relaxing margin when evaluating the acceptability of changes to the CLB.

The level of justification required for changes in margin should depend on how much uncertainty is associated with the performance parameter in question, the availability of mechanisms to compensate for adverse performance, and the consequences of functional failure of the affected elements. Therefore, the

DRAFT FOR COMMENT

results from risk evaluations and the associated analysis of uncertainties, especially in the analysis areas and models affected by the application, will provide useful information to help in the reviewer's decision-making.

In the evaluation of available safety margins, reviewers should also look at the risk profile of the plant. If a proposed CLB change creates or exacerbates a situation where risk is dominated by a few elements (SSCs or human actions) or a few accident sequences, the impact should be carefully evaluated by the reviewer. If one or a few elements clearly dominate risk, then the modeling of these items (including uncertainty) and the effect on risk if they degraded should be reviewed more in detail, and the acceptability of this contribution assessed.

In demonstrating available safety margins, licensees will in some cases 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 the CLB change request:

- to show that a phenomenon of concern cannot occur or is 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 greater than originally assumed.

The reviewer's primary objective is to verify the relevance and acceptability of this new information with respect to the CLB change request. Data that apply 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, the data or analysis must be clearly applicable to the plant and specific circumstances to which it is being applied.

II.3.1.3 Current Regulations

Staff reviewers should be aware that the proposed change satisfies current regulations (including the general design criteria) unless the licensee explicitly includes a proposed exemption or rule change (i.e. a 50.12 "specific exemption" or a 2.802 "petition for rulemaking").

The current licensing basis also applies until modifications to it are accepted by the staff. It is expected that many applications will seek to modify the CLB in risk-informed submittals. Applications that seek to make

DRAFT FOR COMMENT

qualitative changes to the CLB (such as moving components out of the scope of a required program) should be reviewed in more detail with respect to defense-in-depth and safety margins when compared to applications that seek to make parametric changes (such as incremental changes to surveillance interval).

II.3.2 Risk Assessment

For an effective implementation of risk-informed regulatory approaches, the reviewer should ensure that the licensee has demonstrated that the plant's CLB and actual operating conditions and practices are properly reflected in the risk insights using the plant PRA model. Otherwise, the risk assessment may provide inaccurate or misleading information that will require careful scrutiny before use in any regulatory decisionmaking process.

The development of a plant-specific, risk-informed program will also require that information be available to identify the application-specific SSCs and human actions that contribute most significantly to the plant's estimated risk. For each PRA basic event directly affected by the proposed application, it is desirable for the licensee's process to quantify the event using models that capture the functional relationships between the application and the event. The effects of proposed changes on parameters such as common cause failure probabilities and potential increases in human error probabilities should be addressed within the review process.

The characterization of the proposed change in terms of PRA model elements is discussed in sub-section II.3.2.1. The results of this determination of the cause-effect relationships between the proposed application and the PRA models will help define the scope and the level of detail required of the PRA to support the application. Sub-sections II.3.2.2 and II.3.2.3 discuss these topics.

Many applications, such as those involving changes in component test intervals, allow explicit modeling of the impact of the proposed change in the PRA and quantification of the expected change in risk using plausible models of the impact of the change on SSC unavailability to the extent that the affected components are included in the plant PRA. There are other possible risk-informed applications where it may not be feasible to explicitly model the cause and effect relationship because the actual impact on component unavailability resulting from the proposed change is not clearly understood. For applications such as these, the use of risk categorization techniques provide a useful method to identify groups of less risk important SSCs that are possible candidates for a graded approach to regulatory requirements. Using such a categorization approach, it is still necessary to understand the potential or bounding impact of the proposed change, and to assess the risk impact through such bounding evaluations. In either the detailed quantification approach or the risk categorization approach, risk results should be derived from analyses of appropriate quality. The guidelines to help in the review of PRA quality are discussed in sub section II.3.2.4 and

DRAFT FOR COMMENT

also in Appendix A of this SRP. Finally, the issues related to the determination of risk contribution/component categorization are discussed in Appendix C of this SRP.

II.3.2.1 Characterization of Change in Terms of PRA Model Elements

Where quantitative PRA results are used as part of a risk-informed evaluation of a proposed change, the licensee should define the change in terms which are compatible with the risk analysis, i.e., the risk analysis should be able to effectively evaluate the effects of the change.

The characterization of the problem should 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 help define the scope and level of detail of analysis required for the remaining steps of the change-process.

General guidance for the identification of PRA model elements that may be affected by an application is tabulated in Table II-1 of this SRP. 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. The answers to these questions should be used to identify the extent to which the proposed change affects the design, operation and maintenance of plant SSCs.

The reviewer should also verify that the effects of the proposed changes on SSCs are adequately characterized in the PRA elements. For full scale applications of the PRA, this should be reflected in a quantification of the impact on the PRA elements. For applications like component categorization, sensitivity studies on the effects of the change may be sufficient. For other applications it may be adequate to define the qualitative relationship of the impact on the PRA elements or may only require an identification of which elements are impacted.

The review procedure in this element is therefore to verify that the effects of the changes on SSC reliability and unavailability or on operator actions are appropriately 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.

II.3.2.2 Scope of Analysis

The necessary scope of a PRA supporting risk-informed requests will depend on

DRAFT FOR COMMENT

the specific application. 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 should demonstrate that the needed findings are supportable based on traditional engineering analyses, or other plant operational information that address modes and initiators not analyzed in the base PRA.

For plant modes and initiators not analyzed in the PRA such as shutdown, seismic, fire, floods and severe weather, the licensee should consider the effects of the change and provide rationale why additional PRA analyses are not necessary. This rationale could be addressed by assessing the level of redundancy and diversity provided by the plant systems, system trains, human actions, etc. for responding to these unanalyzed configurations. The licensee should also show that the proposed change does not introduce unanalyzed vulnerabilities and that redundancy and diversity will still exist in the plant response capability after the changes are implemented.

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 or remove elements of the plant response capability from programmatic activities aimed at ensuring satisfactory safety performance for plant modes and initiator types not included in the PRA.

OR

- If the proposed change impacts unanalyzed plant modes or initiator types, the licensee demonstrates that a bounding analysis of the change in plant risk from the application (e.g., by qualitative arguments, or by use of sensitivity studies) meets guidelines that are equivalent to the acceptance guidelines specified in Section 2.4.2.1 of draft guide DG-1061.

II.3.2.3 Level of Detail

Generally, the PRA should be detailed enough to account for 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 if the failure of the SSCs that could lead to the initiating events could also result in failure of functions that mitigate that event. For components affected by the application, the

DRAFT FOR COMMENT

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.

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 of the effects of the proposed change on PRA assumptions, screening analyses and boundary conditions.

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 are considered appropriately.
- 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, the mapping will be more complicated.
- If the SSCs are omitted from the model because of inherent reliability or if they are not modeled at all, risk insights on these components should be obtained from an integrated decisionmaking process (such as an Expert Panel) which revisits the assumptions or screening criteria which supported the initial omission.

II.3.2.4 Quality of 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 may provide insights into areas in which existing requirements can be relaxed without

DRAFT FOR COMMENT

unacceptable safety consequences. 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 should be satisfied.

- Reasonable assurance of PRA adequacy: The plant's current licensing basis and actual operating condition and practices are properly reflected in the plant PRA model.
- Robustness of results and conclusions: Results and conclusions must be robust, and an analysis of uncertainties and sensitivities should be carried out to show this "robustness".
- 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 should 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.

Review of PRA Quality

Quality in the licensee's technical analysis must be demonstrated in the licensee request. Guidance in this area is provided in Section 2.7 of DG-1061.

Staff review shall demonstrate that the PRA is of sufficient quality to support the decision. The reviewer should evaluate the licensee process to ensure quality. In addition, for each application, specific findings should be made regarding the quality of the PRA for that application. At a minimum, these findings should be based on a "focused-scope" staff review which will concentrate on application specific attributes of the PRA. This includes a review of the assumptions and elements of the PRA model that drive the results and conclusions.

Appendix A of this SRP provides more detailed guidance on several issues important to the application-specific reviews of probabilistic evaluations performed as part of risk-informed regulation.

In addition to the focused-scope review, the following factors should be considered in determining the need for a more detailed and larger scope staff review of the PRA.

DRAFT FOR COMMENT

- Staff audits of the licensee's 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;
- 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.

Draft NUREG-1602 contains reference material that could be utilized to help in the larger scope staff review of PRAs.

Quality Assurance Requirements Related to the PRA

To the extent that a licensee elects to use PRA as an element to enhance or modify its implementation of activities affecting the safety-related functions of SSCs, appropriate quality requirements will also apply to the PRA. In this context, therefore, a licensee would be expected to control PRA activity in a manner commensurate with its impact on the facility's design and licensing basis. Section 2.7 of DG-1061 provides a description as to what quality elements are applicable to the licensee's PRA activities. The reviewer should determine that the quality of analyses and performance programs which affect safety-related equipment and activities, will meet the quality guidelines as described in draft guide DG-1061.

II.3.2.5 Risk Impact Including Treatment of Uncertainty

Determination of Risk Impact from the Application

For many risk-informed applications, a quantitative estimate of the total impact of a proposed action is expected to be performed. 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 traditional engineering 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 generally needed.

The acceptance guidelines for changes to the plant's risk profile are discussed in section 2.4.2 of draft Reg Guide DG-1061. In the detailed evaluation of risk significance, the following should be considered: baseline

DRAFT FOR COMMENT

risk; change in the baseline risk; and risk in terms of CDF and LERF. 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-scope PRA in all cases.

In accordance with DG-1061, it is expected that applications will result in a net decrease in risk or be risk neutral for plants with CDFs at or above $1\text{E-}4$ per reactor year or LERFs at or above $1\text{E-}5$ per reactor year. In these cases, the reviewer should verify that proposed compensatory measures or plant improvements would clearly offset risk increases from proposed relaxation in current requirements. It is preferred that the net change in risk be quantified, however, risk improvements can also be demonstrated in a non-quantitative sense as long as it can be clearly justified that the risk decrease will at least offset any risk increases.

For plants with base CDFs of less than $1\text{E-}5$ per reactor year and base LERFs of less than $1\text{E-}6$ per reactor year, CDF increase of less than $1\text{E-}6$ per reactor year and LERF increase of less than $1\text{E-}7$ per reactor year is allowed subject to the principles and expectations as specified in Section II.1 of this SRP being met. In the review of where the plant stands in terms of the base risk, the staff should evaluate licensee justification of the base CDF and LERF. For PRAs that are full scope (i.e., those that include all probabilistically significant initiators and operating modes), the review could consist of the verification of PRA quality as described in Section II.3.2.4. For less than full scope PRAs, or in cases where the base risk is close to the acceptance guidelines (e.g., within a half order of magnitude of the guidelines), the reviewer should also consider the licensee's analysis of uncertainties as described later in this section of the SRP. For comparisons in the change in risk, the reviewer is referred to Sections II.3.2.1, II.3.2.2 and II.3.2.3 of this SRP.

In addition to the above guidelines, larger risk increases of $1\text{E-}5$ in CDF and $1\text{E-}6$ in LERF could be allowed subject to increased NRC management review. For this to apply, the base CDF should be less than $1\text{E-}4$ per reactor year and the base LERF should be less than $1\text{E-}5$ per reactor year. In the compilation of information for management review, the staff should include:

- the scope, quality, and robustness of the analysis (including, but not limited to, the PRA), including consideration and quantification of uncertainties;
- the base CDF and LERF of the plant;
- the cumulative impact of previous changes (the licensee's risk management approach);
- consideration of the Safety Goal screening criteria in the staff's Regulatory Analysis Guidelines, which define what changes in CDF and containment performance would be needed to consider potential

DRAFT FOR COMMENT

backfits;

- the impact of the proposed change on operational complexity, burden on the operating staff, and overall safety practices; and
- plant-specific performance and other factors, including for example, siting factors, inspection findings, performance indicators, and operational events.

Treatment of Uncertainties

The uncertainties in the PRA results should be taken into account in the assessment of the risk impact and in the risk-informed decisionmaking process to demonstrate the robustness of the results. The general approach to taking uncertainty into account is discussed in section 2.4.2 of draft guide DG-1061.

When required, the analysis of uncertainties should have the following attributes:

- It should reflect the uncertainties associated with each parameter and provide an assessment of the confidence with which any numerical guidelines are met.
- It should account for model uncertainties. There may be several alternate approaches to the analysis of certain elements of the PRA model. The licensee should document why the model or assumption used is appropriate both for the base case risk evaluation and for the analysis of the impact of the change. In certain cases, it may be necessary to perform sensitivity analyses using alternate models or assumptions to demonstrate the robustness of the conclusions.
- It should attempt to address uncertainty that is caused by potential incompleteness of the scope of the PRA model. The licensee should address the lack of completeness either by demonstrating that the impact of the missing parts on both the base case risk and the change to risk as a result of the application is bounded so that the overall result is acceptable, or by limiting the scope of the application to the SSCs for which the impact on risk can be evaluated (see section II.3.2.2).

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

- review the types and sources of uncertainty that have been identified by the licensee, and how the uncertainties have been addressed with reference to the decision guidelines provided in DG-1061;
- identify if results 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 uncertainties with

DRAFT FOR COMMENT

respect to these elements. (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 acceptance guidelines. The review of the results then should be based on an evaluation of the significance of the hypotheses associated with those modes that exceed the guidelines);

- 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 unanalyzed portion of the risk on both the base case risk and on the change in risk is bounded or can be neglected.

Cumulative and Synergistic Effects from all Applications

The flexibility available to any given plant is not only a function of where it started in terms of base risk, but also a function of how much risk increase has taken place in preceding applications. As discussed in the next section, licensee risk management practices are expected to keep the cumulative increases low. The reviewer is expected to look at past changes in the plant to see if large increases are being accumulated. The reviewer should verify that:

- each application is carried out with reference to a model that already reflects previous applications;
- the cumulative changes from license amendments are being monitored; and
- the accumulation of applications has not created dominant risk contributors.

Beyond cumulative effects, synergistic effects are also possible, not all of which would emerge from a quantification of the PRA. For example, if conventional importance ranking approaches are employed to determine importance of SSCs, it would be possible that multiple requirements could be relaxed on certain "low" significant components under multiple applications. If the QA (potentially affecting the failure rate) and the test interval (potentially affecting fault exposure time) were to be relaxed for the same component, the component unavailability could increase more than expected (since failure rate and fault exposure time combine multiplicatively in the calculation of unavailability). If the effects of QA on failure rate could be quantified convincingly, this would be addressed explicitly, but this cannot presently be assured. As a result, there is potential for different applications to lead to unintended and unquantified synergistic effects on unavailability of a given component.

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

DRAFT FOR COMMENT

consistent with the needed performance with regard to the risk indices and the defense-in-depth concept.

However, it is more straight-forward simply to not allow for the relaxation of multiple programmatic requirements on a given component, unless demonstrable justification is provided that the risk contribution from the component is negligible for 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.

Risk Management

One of the goals of the review should be to ensure that in the course of the licensee's engineering evaluations, principles of risk management are applied appropriately in the process of evaluating changes to current regulatory requirements. For the purposes of this SRP, "risk management" will refer to an approach to decisionmaking about safety that seeks to allocate available resources and worker dose in such a way as to minimize the risk to public health and safety from plant operations. The staff recognizes that there is a point of diminishing returns in risk reduction and that some residual risk will be associated with plant operation, but expects that an effort will be made to identify reasonable measures to control this residual risk as part of the risk-informed regulatory process.

Therefore, as a staff expectation, the process of risk management in risk-informed decisionmaking should not be biased towards elimination of requirements to the exclusion of safety enhancements that would convey a worthwhile safety benefit. Licensees are expected to apply risk insights in an unbiased way, and licensees who do not satisfy subsidiary safety objectives (as defined in DG-1061) are expected to proactively seek safety enhancements in conjunction with any risk-informed applications.

Allowed increases in the CDF and LERF from proposed licensee applications should be small and any increases in the risk should not cause the NRC Safety Goals to be exceeded. The size of an allowable individual risk increase (per DG-1061) depends on the magnitude of the current plant risk. Net increases should generally not be considered without some evidence of licensee effort to identify measures to offset the risk increases caused by the proposed relaxations.

Finally, when risk increases are proposed, reviewers should consider plant performance and past changes to the licensing basis to ensure that there is no pattern for a systematic increase in risk. Insights on the licensee operational practices, management controls, risk management programs, plant configuration control programs, or performance monitoring programs from previous applications can be obtained from the NRC regional offices or from documentation of NRC inspection activities.

11.3.3 Integrated Decisionmaking Process

DRAFT FOR COMMENT

The acceptability of the proposed changes should be reviewed and determined in an integrated fashion. The reviewer should verify that the results of the traditional engineering analyses and the risk assessment have been used to ensure that the principles listed in section II.1 have been met. Due to the scope and quality of the engineering analyses, careful examination of the underlying assumptions in the analyses may be necessary to conclude with reasonable assurance that the principles were satisfied.

As part of the integrated decisionmaking process, implementation and monitoring strategies should be utilized to provide confidence in the results of the underlying engineering analyses. In addition, compensatory measures which reduce risk can be taken to offset incompleteness or uncertainties in the analysis. Compensatory measures can also be used to offset a quantifiable increase in risk with a non-quantifiable but expected improvements in safety.

To ensure that the underlying assumptions utilized in the PRA remain valid, the integrated decisionmaking process should ensure that an appropriate set of programmatic activities (e.g., IST, GQA, ISI, maintenance, monitoring) are maintained for important elements of the plant response capability. In addition, performance of compensating SSCs should be assured (through programmatic activities) when these SSCs are used to help justify the relaxation of requirements of other SSCs.

The process used by licensees to integrate traditional and probabilistic engineering evaluations for risk-informed decisionmaking is expected to be well-defined, systematic, repeatable, and scrutable. Appendix B of this SRP provides review guidance and staff expectations of licensee integrated decisionmaking process.

II.4 Element 3: Develop Implementation and Monitoring Strategies

Implementation and monitoring strategies are important in most risk-informed processes since they can provide early indication of SSC or other plant performance under the proposed changes. In addition, these strategies may be needed to ensure that the key assumptions or performance of key SSCs related to a proposed change are effectively maintained. Section 2.5 of DG-1061 provides guidance for the suggested process in this submittal element.

A key element in the performance monitoring process is the verification of the capability and availability allocated to SSCs which support the underlying basis for the decisionmaking. This process should also include non-safety related SSCs that are relied upon to justify the proposed change to the CLB.

The reviewer should evaluate the implementation and monitoring strategies based on findings of the traditional engineering and probabilistic evaluations.

When broad implementation is proposed over a short period of time, the

DRAFT FOR COMMENT

reviewer should verify that this is consistent with the traditional engineering evaluations, defense-in-depth (including common cause failure) considerations, and risk evaluation models and assumptions. When there is a need to gain additional performance insights given a change in requirements, the reviewer should verify that a phased approach to implementation has been proposed. If this phased approach involves plan implementation for different SSC groups at different times, the basis for the selection of the SSC groups and the timing should be reviewed.

When SSC or licensee performance can be affected by the proposed change, the reviewer should ensure that monitoring strategies are proposed to evaluate the performance over a period of time. This monitoring should be based on the reliability/availability and key modeling assumptions allocated to SSCs in the risk model (or on performance of operators, where appropriate) used to support the proposed change in regulation. As such, the reviewer should ensure that performance criteria chosen are consistent with the level of performance allocated in the risk analysis.

When monitoring that is already being performed as part of the Maintenance Rule implementation is also proposed for the current application, the reviewer should ensure that the performance criteria chosen are appropriate for the application in question.

Licensee proposed corrective actions should also be reviewed as part of the review on the monitoring program. If monitoring detects degradation, then there should be provisions for the SSCs to be refurbished, replaced, or tested/inspected more often (or a combination of these initiatives). The selected action should be based on a root cause analysis 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 phased implementation are lost). One approach to ameliorate this concern would be to obtain performance data of similar SSCs at other plants with a range of operating times to expand the applicable database over a range of component ages. Such a program would be expected to provide a 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.

DRAFT FOR COMMENT

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.

II.5 Element 4: Staff Evaluation of Submittal

In order for the staff to make a conclusion of acceptability of the proposed CLB change based on review guidance provided in earlier sections, sufficient engineering and licensing information have to be submitted or be made available by the licensee. Furthermore, the data, methods, and assessment criteria used to support the regulatory decisionmaking should be available for public review.

In addition, appropriate regulatory action should be requested by the licensee. Requests for proposed changes to the plant's CLB typically take the form of requests for license amendments (including changes to or removal of license conditions), technical specification changes, changes to or withdrawal of orders, and changes to programs pursuant to 10 CFR 50.54 (e.g., QA program changes under 10 CFR 50.54(a)). The staff should determine if: (i) the form of the change request is appropriate for the proposed CLB change; (ii) the information required by the relevant regulation(s) in support of the request is submitted; and (iii) the request is in accordance with relevant procedural requirements. For example, license amendments should meet the requirements of 10 CFR §§50.90, 50.91 and 50.92, as well as the procedural requirements in 10 CFR §50.4. Where the licensee submits risk information in support of the CLB change request, that information should meet the guidance in Section 3 of draft guide DG-1061.

Licensees have a choice of whether to submit results or insights from risk analyses in support of their CLB change request. Where the licensee's proposed change to the CLB is consistent with currently-approved staff positions, the Staff's determination will be based solely on traditional engineering analysis without recourse to risk information (although the Staff may consider any risk information which is submitted by the licensee). However, where the licensee's proposed change goes beyond currently-approved staff positions, the Staff should consider both information based upon traditional engineering analysis as well as information based upon risk insights. If the licensee does not submit risk information in support of a CLB change which goes beyond currently-approved Staff positions, the Staff may request that the licensee provide this information. Such a request is not a backfit under 10 CFR 50.109. If the licensee chooses not to provide the risk information, the Staff will review the proposed application using traditional engineering analysis and determine whether sufficient information has been provided to support the requested change.

In risk-informed change proposals, licensees are expected to identify SSCs with high risk significance which are not currently subject to regulatory

DRAFT FOR COMMENT

requirements, or are subject to a level of regulation which is not commensurate with their risk significance, and propose CLB changes that will subject these SSCs to the appropriate level of regulation, consistent with the risk significance of each SSC. Specific information on the staff's expectation are set forth in the application-specific regulatory guides. The staff reviewer should assure that the application-specific guidance is followed. If there is no guidance, the reviewer should determine whether any assumptions from the risk analysis are reflected in the licensing basis, and that commitments for enhanced regulatory requirements/controls applicable to high risk SSCs not currently subject to regulatory requirements (or subject to a level which is not commensurate with their risk significance) are appropriate and reflected in the licensing basis.

Update of the Safety Analysis Report

Reviewers should assure that the proposed changes, when approved by the staff, will be appropriately included in future updates to the licensee Safety Analysis Report. In addition, important assumptions including SSC functional capabilities and performance attributes, which play a key role in supporting the acceptability of the CLB change, should be identified by the licensee. Since the continued satisfaction of these assumptions is necessary to maintain the validity of the safety evaluation, the reviewer should verify that such assumptions are reflected by licensee commitments which are incorporated into the Safety Analysis Report. The reviewer should verify that the licensee has submitted revised FSAR pages as necessary. This revision should include all the programmatic activities, performance monitoring aspects and SSC functional performance and availability attributes which form the basis of the request. This material should identify those SSCs whose performances should be verified (including nonsafety-related SSCs whose performance and reliability provide part of the basis for the CLB change).

NEPA Considerations

In accordance with 10 CFR Part 51, environmental protection regulations such as those from the National Environmental Policy Act (NEPA) would have to be addressed as part of the staff's review process. The reviewer should utilize NRR Office Letter 906, Revision 1 and 10 CFR 51.25 to determine how the NEPA requirements are to be addressed. If it is determined necessary, an environmental assessment (EA) should be prepared to assess whether an environmental impact statement (EIS) is required or whether a finding of no significant impact (FONSI) can be made. It is expected that, if all the guidance and acceptance criteria provided in DG-1061 is satisfied, the staff should normally be able to make a finding of no significant impact for the proposed CLB change.

Table II-1 (page 1 of 3)

Questions to Assist in Establishing the Cause-Effect Relationship²

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 affect 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 affect CCF probabilities?

² Information from section 3.3 of the EPRI PSA Applications Guide provided substantial input to this listing.

DRAFT FOR COMMENT

Table II-1 (page 2 of 3)

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 should 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)?

DRAFT FOR COMMENT

Table II-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 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 or to the other portions of the containment?
- 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?
- 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. EVALUATION FINDINGS

The results of a reviewer's evaluation should reflect a consistent and scrutable integration of the probabilistic considerations and traditional engineering 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, defense-in-depth and sufficient safety margins are maintained. Findings of acceptability should be supported with logical bases built from an evaluation of the considerations given in section II.

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

General

- The proposed change meets the current regulations. This principle applies unless the proposed change is explicitly related to a requested exemption or rule change (i.e., a 50.12 "specific exemption" or a 2.802 "petition for rulemaking").
- Defense-in-depth is maintained.
- Sufficient safety margins are maintained.
- Proposed increases in risk and their cumulative effect are small, and these changes do not cause the NRC Safety Goals to be exceeded.
- Performance-based implementation and monitoring strategies are proposed that address uncertainties in analysis models and data and provide for timely feedback and corrective action.
- All safety impacts of the proposed change are evaluated in an integrated manner as part of an overall risk management approach in which the licensee is using risk analysis to improve operational and engineering decisions broadly and not just to eliminate requirements the licensee sees as undesirable. The approach used to identify reduced requirements was also used to identify if there are areas where requirements should be increased.
- The acceptability of the proposed changes have been evaluated in an integrated fashion that ensures that all principles are met;
- Increases in estimated CDF and LERF resulting from proposed CLB changes are limited to small increments.

DRAFT FOR COMMENT

- The scope and quality of the engineering analyses (including traditional and probabilistic analyses) conducted to justify the proposed CLB change are appropriate for the nature and scope of the change and are based on the as-built and as-operated and maintained plant.
- Appropriate consideration of uncertainty has been given to analyses results and interpretation of findings.
- The plant-specific PRA supporting licensee proposals has been subjected to quality controls such as an independent peer review.
- Data, methods, and assessment criteria used to support regulatory decisionmaking are available for public review.

Definition of the Proposed Change

- Adequate traditional engineering and probabilistic evaluations are available to support the proposed CLB change. Plant-specific and relevant industry data and operational experience also supports the proposed change.
- Cause-effect relationships have been identified to adequately link the application with the PRA model elements.
- The proposed risk models can effectively evaluate or realistically bound the effects of the proposed change.
- Information from engineering analyses, operational experience, plant-specific performance history have been factored into the decision process.

Evaluations of Defense-In-Depth Attributes and Safety Margins

- Defense-in-depth is preserved, for example: system redundancy, diversity and independence is maintained commensurate with the expected frequency and consequence of challenges to the system; defenses against potential common cause failures are maintained and the introduction of new common cause failure mechanisms is assessed; and defenses against human errors are maintained.
- Sufficient safety margins are maintained, for example: codes and standards approved for use by the NRC are met or deviations justified; and safety analysis acceptance criteria in the CLB are met, or proposed revisions provide sufficient margin to account for analysis and data uncertainty.
- Current regulations have been met or the proposed exemption is acceptable.

DRAFT FOR COMMENT

Scope of Risk Analysis

- The licensee's PRA satisfactorily addresses all mode/initiator combinations, **OR**
- The licensee's PRA does not need to analyze the following mode/initiator type combinations. [List combinations] In each instance, the licensee has demonstrated that:
 - suitably redundant and diverse plant response capability is maintained for significant initiators in these modes; and
 - sufficient elements of the plant response capability are subject to programmatic activities to assure suitable performance.

Level of Detail of Risk Analysis

- The PRA is detailed enough to account for important system and operator dependencies.
- Risk insights are consistent with the level of detail modeled in the PRA.

Quality of the PRA

- There is reasonable assurance of PRA adequacy as shown by the licensee process to ensure quality and by a focused 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 licensee commitments.

Risk Impact and Treatment of Uncertainty

- If the risk-informed application is based on the quantification of the change to risk, then the following applies:
 - 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 guidelines defined in draft guide DG-1061. The cumulative and synergistic effects on risk from the present and previous applications have been addressed. Licensee risk management practices are being followed to minimize the risk from plant operations.

DRAFT FOR COMMENT

- In either of the above cases, 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.
- If the risk-informed application is based on a qualitative assessment of the change to risk, then the application is shown to result in a decrease in plant risk, or is risk neutral, or CDF and LERF increases are shown to be acceptable based on bounding evaluations or sensitivity studies. When this assessment is based solely on traditional engineering information or use of compensatory actions, then the application clearly shows a reduction in risk.

Integrated Decisionmaking Process

- Results from traditional engineering analyses and risk analyses have been used to ensure that the principles for risk-informed decisionmaking have been met.
- Potential analysis limitations, uncertainties and conflicts are resolved by use of conservative results, or by use of appropriate implementation and monitoring strategies, or by use of appropriate compensatory measures.
- The integrated decisionmaking process is well-defined, systematic, repeatable, and scrutable.

Implementation and Monitoring Strategies

- The implementation process is commensurate with the uncertainty associated with the results of the traditional 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 corrective action plan will assure that appropriate actions can be taken before SSC functionality and plant safety is compromised. Data from similar plants will be used if needed.
- In addition to the tracking of performance of SSCs affected by the application, the performance monitoring process also includes the tracking of performance of SSCs which support the underlying basis for the decisionmaking.

DRAFT FOR COMMENT

Licensee Submittal

- The submittal includes sufficient information to support conclusions regarding the acceptability of the proposed change.
- The appropriate regulatory action was requested. In addition, pertinent information on the CLB change will be included in the Safety Analysis Report, technical specifications or license conditions as necessary.
- The licensee has appropriately committed to the important programmatic and performance assumptions in the PRA and engineering analyses which served as the basis of the CLB change. These include any enhancements to regulatory requirements necessary to preserve assumptions in the PRA and engineering analyses, and to reflect new regulatory requirements for high risk significant SSCs not otherwise subject to existing requirements, commensurate with their risk significance. These commitments are reflected in revisions to the Safety Analysis Report, technical specifications or appropriate licensee conditions have been imposed by the staff.

IV. 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 demonstrating that a proposed CLB change is acceptable, the method described herein will be used by the staff in its evaluation of risk-informed changes to the CLB.

DRAFT FOR COMMENT

V. 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. "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis," Draft Regulatory Guide, DG-1061, XXXXX, 1997.
6. "Guidelines for Use of PRA in Risk-Informed Applications", Draft NUREG-1602, XXXXX, 1997
7. "Procedures for Treating Common Cause Failures in Safety and Reliability Studies", NUREG/CR-4780, January 1988
8. "Severe Accident Risks: An Assessment for Five Nuclear Power Plants," NUREG-1150, Volumes 1 and 2, December 1990
9. "Common-Cause Failure Data Collection and Analysis System", Draft Volumes 1 through 6, INEL-94/0064, December 1995

Appendix A

GUIDANCE FOR A FOCUSED-SCOPE APPLICATION SPECIFIC PRA REVIEW

As stated in Section II.3.2.4 of this SRP and in draft guide DG-1061, PRAs that are used in risk-informed submittals to determine risk significance or risk impact should have been shown to be of adequate quality. Staff evaluation of a licensee risk-informed application submittal is expected to include a review of the licensee process for PRA quality assurance. Where necessary, this should be supplemented by an overall review of the following: event and fault tree models; data on SSC failures and common cause failures; mission success criteria; initiating event analysis; human reliability analysis; and result quantification including the analysis of uncertainties. These reviews should be of sufficient detail to provide the staff with confidence that the PRA properly reflects the plant's CLB and actual operating conditions and practices. Results from previous staff review efforts (e.g., from prior applications) should be utilized as appropriate.

In addition to the general overall review as described above, staff reviewers are also expected to perform a focused-scope review of the risk analysis on an application-specific basis. This appendix provides review guidance on the likely elements of a PRA which may affect or be affected by proposed changes to the CLB.

A.1 Use of Appropriate Data

a. Area of Review

In risk-informed applications it is important that appropriate SSC failure data is used. While plant-specific data is preferred, for plants with little operating history, the only choice is use of generic data. Furthermore, when the impact of the change is being modeled as a modification of parameter values, there may be no plant-specific data to support the modification. The data related issues are the following: a) if the impact of the application is to be modeled as a change in parameter values associated with basic events representing modes of unavailability of certain SSCs, these changes should be reasonable and should be supported by technical arguments; and b) the impact of the change is neither exaggerated nor obscured by the parameter values used for those SSCs unaffected by the change.

b. Review Guidance and Procedures

It is to be expected that, for a PRA that has undergone a technical review, parameter values will have been judged to be appropriate, whether they have been evaluated using generic or plant specific data. However, since the review was focused on the PRA as a base case model, a different perspective on the appropriateness of parameter values may be required for specific applications. Therefore, in reviewing PRA applications, the reviewer should focus on those parameter values that have the potential to change the

DRAFT FOR COMMENT

conclusion of the analysis. For example, parameters associated with SSCs that appear in the same cutsets as the affected SSCs have the potential to distort the conclusions by decreasing the assessed importance of the change if their values are too low, or by increasing it if their values are too large. Similarly, parameters that contribute to the cutsets that do not contain affected SSCs can decrease the importance of the change by being too large, or increase it by being too low.

Whether the data used is plant-specific, generic, or a combination of both, the parameter values are expected to be consistent with generally accepted values from PRAs of similar plants, or significant deviations should have been justified. Significant in this context can be defined as no greater than a factor of 3 for the mean values of the failure rate or failure probability. The focus of the review should be on those parameter values which both have a significant impact on the results as discussed above, and which deviate significantly from the generally accepted norm.

If it was decided that a more detailed review of the parameter values is appropriate, then the following guidance applies. For plant-specific data, the reviewer should determine how plant records were used to estimate the number of events/failures, the number of demands, and the operating hours or standby hours. The reviewer should verify the consistency between the definitions of failure modes and component boundaries used in the risk analysis and the definitions used in the plant records. When generic data are used, it is important to verify that the plant component is typical of the generic industry component. In cases where generic failure rates are used in combination with plant-specific data like test intervals, the reviewer should verify that the generic data are applicable for the range of plant data used.

When evaluating the impact of the change, it is important for the reviewer to recognize the assumptions that have gone into developing the PRA model. For example, two models are commonly used for events representing the unavailability of a standby component on demand; the standby failure rate model and the constant probability of failure on demand model. Using the former model can result in large differences between the unavailabilities of components whose test intervals differ significantly, given the same standby failure rate is used. The reviewer should be sensitive to this effect, and ascertain that appropriate models are used. As another example, in considering plant-specific failure data, poorly-performing individual components may have been grouped with other components, allowing their poor performance to be averaged over all components of that type. Poor performance may arise because of inherent characteristics of one member of what would otherwise be considered a uniform population, or may arise because components are operating in a more demanding environment. If these components are grouped together with others for which the operating conditions are more favorable, then the failure rates used for the poor performers could be artificially lowered. If requirements are relaxed based on the group failure rate, reduced programmatic attention to these poor performers could lead to a greater than expected probability of experiencing an in-service failure of one

DRAFT FOR COMMENT

of these components. The reviewer should be aware of such effects, and should make sure that components are grouped appropriately.

When the impact of the change is being modeled as a change in the parameter values associated with specific basic events representing modes of unavailability of SSCs, the reviewer should focus on whether the change in parameter values is appropriate and reasonable. The rationale behind the change in parameter values is expected to be documented and should be reviewed carefully.

If generic values are used for the base case parameter values which are candidates for being changed, it should be checked that the conditions under which the generic data are applicable do not correspond to those which would be more appropriate for a plant with the change incorporated. This should only be a real concern if the plant being changed is somewhat untypical with respect to the issue being addressed by the change. This would not be a concern if plant specific data were being used.

Finally, as a validation of the data used to justify CLB changes in risk-informed applications, monitoring of the performance of components affected by the application is important. This monitoring should be performed as the proposed application is phased in. For very reliable SSCs, it may be necessary for the licensee to review available operating experience at other plants for applicability to the licensee's plant to expand the operating experience database. The reviewer should ascertain that the monitoring program is capable of demonstrating that the performance of the components or systems is in accordance with what has been assumed.

c. Evaluation Findings

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

- The failure rates and probabilities used, especially those that directly affect the proposed application, appropriately consider both plant-specific and generic data that are consistent with generally accepted values from PRAs of similar plants, and deviations (if any) have been justified.
- The licensee has systematically considered the possibility that individual components could be performing more poorly than the average associated with their class, and have avoided relaxation for those components to the point where the unavailability of the poor performers would be appreciably worse than that assumed in the risk analysis.
- The changes to the parameter values impacted by the application are both justified and reasonable.
- Data used to support changes to the CLB are supported by an appropriate

DRAFT FOR COMMENT

performance monitoring program.

A.2 Initiating Events

a. Area of Review

Whether or not a particular initiating event is included in a PRA depends on the scope of the PRA, the frequency of that event, the available plant systems or other features to mitigate the event, and the consequences of the event if unmitigated. Proposed plant changes could affect the frequency of initiating events, the probability of mitigation of event initiators and, in some cases, event consequences. In addition, plant changes could potentially introduce new initiating events or result in previously screened out events becoming more important.

b. Review Guidance and Procedures

For risk-informed applications, the staff should determine if initiating events and anticipated plant response are affected by the proposed changes. The reviewer should determine if the proposed changes: (i) can lead to an increase in the frequency of an initiator already included in the PRA; (ii) can lead to an increase in the frequency of an initiator initially screened out in the PRA; (iii) have the potential to introduce new initiating events; and (iv) can affect the grouping of initiating events. These are discussed further below.

Applications that result in changes to initiator frequency or the ability of the plant to respond to event initiators are relatively easy to model in the risk analysis if the initiators are already included in the base analysis. In these cases, the impact of the changes should be evaluated directly from the risk model.

In cases where initiators are not included in the original risk analysis based on screening evaluations, it is necessary to review whether initiating events previously screened out on grounds of low frequency, might now be above the screening threshold as a result of a proposed application. Plant changes could increase the frequency of initiating events that were relatively infrequent to begin with, or these changes could affect SSCs or operator actions that were credited with the satisfactory mitigation of initiating events. If initiating events increased in frequency as a result of an application to the point where it became important (i.e., could no longer be screened out), then the scope of the analysis would need to change to reflect this.

Usually, low frequency of an event by itself is not sufficient as a criterion for screening purposes. The consequences of non-mitigation of the events also play a big part in this process. For example, interfacing system LOCAs are often assessed as low frequency events, but because of their impact on public

DRAFT FOR COMMENT

health and safety, they can be important. Therefore, for potentially high consequence events, even if the event frequency is below a screening criterion, the features that lead to the frequency being low (for example, surveillance test practices, startup procedures, etc.) should be taken into account in reviews of PRA applications.

Proposed plant changes should be evaluated to determine if these changes could result in initiators not previously analyzed in the PRA. For example, changes might enhance the potential for spurious operation of components whose action may cause initiating events or changes might increase the likelihood for operator errors of commission which may result in plant trips. If mechanisms for producing new initiators have been identified, the reviewer should make sure that they have been added to the risk analysis so that the impacts from these initiators can be analyzed.

In PRAs, initiating events are usually grouped according to the systems required to respond to the transient. This implies that success criteria for plant systems and operator response are similar for all events in a group. In addition, events may be screened out when it can be shown that they are bounded in probability and consequence by other similar events. In the review of risk-informed applications that affect initiating events, the staff has to ensure that grouping criteria used in the base analysis have not been invalidated by the proposed plant changes or, in the case where this is not true, the licensee has made appropriate changes to the event groupings.

Finally, it should be noted that many PRAs model initiating events as single basic events or "black boxes". In risk-informed regulation, it is preferred that initiating events especially those that result from the loss of support systems, be modeled using a fault tree (or equivalent) approach so that system dependencies are fully understood and accounted for. If this is not the case, the reviewer should be aware of the combination of SSC failures or other events that could lead to the "failure" of the black box. This would lead to a better understanding of the risk contributors and is especially important in risk categorization applications.

c. Evaluation Findings

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

- The licensee has adequately considered the effects of proposed changes on the frequencies of initiating events analyzed and the frequencies of initiating events previously screened out.
- The changes have been shown to not result in new initiating events, or if new initiators are identified, these have been added to, and analyzed in the risk model.
- Proposed changes have been taken into account in the grouping of

initiating events.

- Dependencies between the initiating events and the plant mitigation systems have been considered in the decisionmaking process.

A.3 Determination of Success Criteria

a. **Area of Review**

Guidance in the PRA policy statement and in DG-1061 stipulates that realistic analysis should be used in PRA implementation. The following discussion is aimed at sorting out what is meant by "realistic" 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 for the initiating event considered.

Applying the SAR mission success criterion in a PRA would be conservative, in the sense that the probability of failure to meet this standard of performance would be greater than probability of failure to meet a more realistic standard of performance. However, re-analyzing event sequences with conventional SAR tools would be too burdensome to apply to the large number of scenarios that are defined in the course of a PRA. In addition, the rather specialized computer codes used in SAR analysis may not be appropriate in beyond-single-failure scenarios. Traditionally, development of mission success analysis in PRAs has ranged from the use of faster running models that might not have the same level of quality assurance as the conventional SAR tools, to the extrapolation of results from analysis performed on similar plants.

In order to satisfy the Commission guideline, then, the staff should 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 changes to the CLB have a sound technical basis.

b. **Review Guidance and Procedures**

When it is determined that the results and conclusions of a risk-informed application are especially sensitive to the choice of mission success criteria, or if the modeling is particularly controversial, the staff should review the relevant success criteria and the basis for each. In cases where the basis is lacking, the reviewer should either request additional licensee justification or seek independent analysis.

DRAFT FOR COMMENT

If the basis is analytical, staff evaluation of the code used and the input data may be appropriate. When it is determined that the computer codes used have not received adequate licensee or other industry review, then closer examination of the models should also be considered.

The models, codes, and input used to determine mission success criteria should meet QA standards that are consistent with general accepted methods. This 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 should be explicit (i.e., engineering calculations and codes should be verified and quality assured) and it should be formalized by the licensee as part of the licensee QA program.

Some mission success criteria can validly be extrapolated between similar plants when a firm basis for the criterion is created at the first plant and it is shown that plant-specific features do not invalidate the comparison.

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 reviewer should assure that the success criteria are not optimistic so as to underestimate the number of components required (i.e., overestimate the size of the minimal cutset).

c. Evaluation Findings

In cases where conclusions are sensitive to the mission success criteria, the staff safety evaluation report should contain findings equivalent to the following:

- a technical basis has been established for the mission success criterion used in the analysis. Analytical elements of the technical basis have been given an appropriate level of configuration control and quality assurance. Where comparison with analogous criteria from other plants is possible, this comparison has been justified.

A.4 Modeling of Common Cause Failures

a. Area of Review

Common cause failures (CCF) represent the failures of components that are caused by common influences such as design, manufacturing, installation, calibration or operational deficiencies. Since CCFs can fail more than one component at the same time and can occur with greater probability than would be predicted by the product of the individual component failure probabilities, they can contribute significantly to plant risk.

Risk-informed applications that cover SSCs as a group have the potential of

DRAFT FOR COMMENT

affecting the CCF probabilities of SSCs within that group. For the affected components, CCF probabilities could be low or might not even be included in the baseline PRA models based on the operational and engineering evidence driven by current requirements. With proposed changes there should be assurance that the CCF contribution will not become more significant. In addition, the assessment of the impact of the change can be affected by the CCF probabilities for other components, and can either be exaggerated or obscured depending on the CCF probabilities.

b. Review Guidance and Procedures

The reviewer should verify that potentially significant CCFs have been covered in the PRA and that, where applicable, the effects of the proposed changes have been incorporated into the CCF modeling. Staff evaluation should include a review of the process used for the selection of common cause component groups.

Acceptable methods for the modeling of CCF contributions are presented in NUREG-4780 (reference 7). Additional guidance can be found in an AEOD report "Common Cause Failure Data Collection and Analysis System"-(reference 9), which also provides an extensive database of generic CCF probabilities that can be used to compare to those used in the risk-informed licensee submittal. Significant differences in CCF probabilities should be reviewed carefully to determine whether they are justified.

Specific review guidelines related to risk-informed applications and the assessment of the change are provided below.

- 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 risk model where appropriate.
- For relevant applications, reviewers should check that licensees have appropriately modeled CCF of groups of equipment that were proposed for the change. In cases where the effects of the application on CCF cannot be easily evaluated or quantified, reviewers should establish that performance monitoring is capable of detecting CCF before multiple failures are likely to occur subsequent to an actual system challenge. In addition, to reduce fault exposure times for potential common cause failures, phased or incremental implementation should be considered as part of the effort to protect against CCF.
- The reviewer should make sure that the impact of the change is not inappropriately made insignificant by the choice of CCF probabilities for SSCs unaffected by the change. This can occur in two ways. First, the cutsets containing events which represent failures of SSCs affected by the change may include CCF contributions from other SSCs which are too small. Second, the cutsets which do not contain affected SSCs may

DRAFT FOR COMMENT

be artificially increased in value by having CCF contributions that are too large so that the impact of the change is obscured. These cases will impact applications involving risk categorization by lowering the relative contribution (and importances) of the affected SSCs. An understanding of these effects can be obtained from sensitivity analyses performed by removing the pertinent CCFs or by using more realistic values for the CCFs.

- A common modeling approximation is to include CCF contributions only from that combination of SSCs which fails the function of the system. For example, if system success is defined as success of 1 out of 4 components, usually only a single term representing a CCF of all four components is included. If the success criterion were 2 out of 4, the corresponding CCF term would represent failure of any three or all four SSCs in the group. While probabilistically this usually corresponds to the dominant contributions, care has to be taken when the application relies on assessing the impact on risk of having one train unavailable. In this case, the effective success criterion of the remaining part of the system changes, so that in the case of the 1 out of 4 system, a CCF of three SSCs becomes a possible contributor. The impact of not modeling the lower order CCF contributors should be investigated. Note that this can impact applications for which the justification of the change relies on risk categorization as well as those that require an evaluation of changes to risk.

c. 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 component groups sharing attributes that correlate with CCF potential and that affect the application.
- Where applicable, the licensee's performance monitoring program addresses a phased implementation approach to reduce the potential for increased incidence of CCFs due to the proposed change.

A.5 Modeling of Human Performance

a. Area of Review

The results of a PRA, and therefore the input it provides to risk-informed decisionmaking, can be very strongly influenced by modeling of human performance. Plant safety depends significantly on human performance, so it is essential that PRAs treat it carefully. However, the modeling of human performance, typically referred to as Human Reliability Analysis (HRA), is a relatively difficult area; significant variations in approach continue to be encountered, and these can result in significantly different estimates of

DRAFT FOR COMMENT

human error probabilities (HEPs) for what appear to be similar human failure events. The particular values used for HEPs can significantly influence results of the assessment of the impact of a proposed change. In addition to the quantification issue, there are 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. One further issue is the impact of human performance which is not explicitly modeled, but is implicit in certain parameter values. An example is the influence of human performance on initiating event frequency. The causes of initiating events are typically not addressed; their impact is included in the frequency in an implicit way.

b. Review Guidance and Procedures

The reviewer should have an understanding of the potentially significant human performance issues that might be affected by the application and how these are reflected in the PRA. This should include a review of the approach used to estimate human error probabilities. The human errors probabilities can impact the assessment of the change in one of three ways. First, HEPs unrelated to the change can obscure or exaggerate the impact of the change depending on their values by inappropriately increasing or decreasing the value of the cutsets unaffected by the change. Second, the HEPs may represent responses to failures of the SSCs impacted by the change. Third, the HEPs may be directly affected by the change.

Specific guidance related to the assessment of the impact of the change is provided below.

- The reviewer should make sure that the impact of the change is not inappropriately made insignificant by the choice of HEPs included in the PRA model. This can occur in two ways. First, the cutsets containing events which represent failures of SSCs affected by the change may include HEPs which are too small. Second, the cutsets which do not contain affected SSCs may be artificially increased in value by having HEPs that are too large so that the impact of the change is obscured. These cases will impact applications involving risk categorization by lowering the relative contribution (and importances) of the affected SSCs. An understanding of these effects can be obtained from sensitivity analyses performed by removing the pertinent HEPs or by using more realistic values for the HEPs.
- The reviewer should identify any human actions that compensate for events affected by the proposed application, and ensure that

DRAFT FOR COMMENT

inappropriate credit has not been taken for these events.

- Justification of proposed changes to the CLB that are based on taking credit for post-accident recovery of failed components (repair or other non-proceduralized manual actions, such as manually forcing stuck valves to open) should be reviewed carefully to ascertain whether the identified recovery action is an obvious one to take, and is feasible given the time and physical constraints.

Credit may be taken for proceduralized implementation of alternative success strategies to work around a failed component. Licensees that take this kind of credit should demonstrate that these recoveries are feasible and are supportable by plant programs such as training, etc.

- For human actions that are used to compensate for a basic event probability increasing as a result of proposed CLB changes, licensee actions to ensure operator performance at the level credited in the risk analysis should also be a part of the CLB change.
- For human actions that represent responses to the unavailability of SSCs which are impacted by the change, an assessment should be made on whether the conditions under which the human actions are to be performed have changed significantly so that the HEP should be modified.
- For HEPs that are directly impacted by the change, e.g., as a result of a procedure or operating practice, the reviewer should make sure that the impact has been modeled appropriately. In particular, care should be taken to check whether HEPs that have been screened out of the model should now be reinstated.
- The reviewer should assess whether any dependencies between HEPs have been altered by the change.
- The reviewer should be assured that the set of HEPs used in the PRA is internally consistent, and that the proposed changes, if any, are made consistent with the changes in the performance shaping factors (PSFs) used by the analysts.

c. Evaluation Findings

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

- The modeling of human performance is appropriate.
- Post-accident recovery of failed components is modeled in a defensible way. Recovery probabilities are quantified realistically. The formulation of the model shows decisionmakers the degree to which the apparently low risk significance of certain items is based on credit for

DRAFT FOR COMMENT

recovery of failed components (restoration of component function, as opposed to actuation of a compensating system).

- When human actions are proposed as compensatory measures as part of a proposed CLB change, licensee actions to ensure operator performance at the level credited in the risk analysis (e.g., by training, procedures, etc.) are also a part of the CLB change.

A.6 Effects of 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. Review Guidance and Procedures

Acceptability of a truncation value used in the baseline PRA should be reviewed as part of the licensee review process. On an application specific basis, licensees should also demonstrate and reviewers should verify 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.

It is preferred that the change in risk from the application is calculated 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 an application. If model requantification was not performed or if the application depended on the risk ranking of SSCs from a pre-solved cutset equation, the reviewer should use the guidelines provided below.

The reviewer should be assured (either by documentation provided in the licensee review or by an independent analysis) that cutset truncation has not introduced errors into the application results or the logic of the PRA that affect the application. 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.

DRAFT FOR COMMENT

Staff review could also include a comparison of a list of the events affected by the application that is in the final truncated cutset equations to the list of application-specific basic events used in the 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 that enables the reviewer to determine the reason truncated events are not important to the risk.

Finally, 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 verify 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, or human dependencies are considered.

c. Evaluation Findings

The staff review should conclude that the licensee has satisfactorily established that conclusions are not adversely affected by truncation, i.e.,

- the truncation criteria is sufficiently low to ensure stable results, that is, 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 can demonstrate the reasons why they are unimportant to risk.

DRAFT FOR COMMENT

Appendix B INTEGRATED DECISIONMAKING

Risk-informed applications are expected to require a process to integrate traditional engineering and probabilistic considerations to form the basis for acceptance. In order for this decisionmaking process to be effective in rendering accurate representations of plant safety and risk, it is expected that documented guidance be available to ensure consistent and defensible results. Such guidance would also allow staff reviewers to reconstruct the logic and events involved in the integration process.

This appendix discusses issues that should be addressed by the staff during reviews of the licensee integrated decisionmaking process (sometimes referred to as the "expert panel" process by licensees).

a. Area of Review

Staff reviewers are expected to evaluate all proposed changes to the CLB taking into account both traditional and probabilistic engineering considerations. For each proposed change, the reviewer should evaluate the licensee justification for the change. In cases where licensee results or conclusions are in some way counter-intuitive or inconsistent with results for similar plants on similar issues, the reviewer may also want to evaluate in detail the licensee documentation of the process by which the results were obtained. This would provide a better understanding of the reasons, assumptions, approaches, and information that were used in the licensee integrated decision process.

b. Review Guidance and Procedures

Since the licensee integrated decisionmaking process is responsible for the justification of acceptability of the proposed changes to the CLB, it is expected that the process will be documented in a relatively formal fashion. The staff may not routinely audit all of the licensee findings or recommendations, but the documentation should exist to support such a review, and should be maintained for the life of the plant or until such time when the recommendations are invalidated by later changes.

Staff expectations of the integrated decisionmaking process:

- The process should be well-defined, systematic, repeatable, and scrutable. This process should be technically defensible and should be detailed enough to allow an independent party to reproduce the major results.
- Deliberations should be application specific. The objectives proposed for the integrated decisionmaking process for a particular application (particularly, how the results are to be utilized) should be well defined and should be relevant to that application.

DRAFT FOR COMMENT

- Membership in the decisionmaking team should include experienced individuals with demonstrated skills and knowledge in relevant engineering disciplines (depending on the application), plant procedures and operations, system knowledge including operational history, system response and dependencies, operator training and response, details of the plant specific probabilistic risk assessment, and regulatory guidance.
- The decisionmaking team should have been advised of the specifics of all proposed changes and the relevant background information associated with the licensing action. In addition, since the judgement will be based in part on the results of a risk analysis, imparting to the team an interpretation of the results of the risk model and the potential limitations of this model is important.
- The process should take into account the principles and the NRC expectations as described in Section 2.1 of DG-1061.
- In the formulation of findings, both probabilistic and traditional engineering considerations should be taken into account. This should include information from the risk analysis, traditional engineering evaluations and insights, quantitative sensitivity studies, operational experience and historical plant performance, engineering judgment, and current regulatory requirements. Potential limitations of the risk model should be identified and resolved. SSCs that are affected by the proposed application but that are not modeled in the PRA should be considered individually and evaluated based on guidelines similar to those provided later in this appendix or in appendix C.2. Finally, conclusions should be robust to different plausible assumptions and analyses.
- When findings or conclusions are based in part on the use of compensatory measures, justification should be provided as to why the compensatory measures are an appropriate substitute for a proposed relaxation in current requirements. The compensatory measure should become part of the plant licensing basis.

Technical information basis:

In many risk-informed pilot applications, integrated decisionmaking panels have been utilized in cases where there are broad applications of PRA and traditional engineering results over a large number of plant SSCs to justify changes to the CLB. In cases such as these, it is expected that the information base supplied to the integrated decisionmaking panel is capable of supporting the findings that should be made in the context of the specific risk-informed application. For example, in risk quantification and risk categorization type of applications, the following should be applicable.

DRAFT FOR COMMENT

- At least the level 1 portion of the internal events PRA should be formulated in such a way as to support quantification of a change in risk (Δ CDF and Δ LERF) and importance measures, and should provide qualitative (minimal cutset) information adequate to support defense-in-depth findings.
- There should be an inventory of plant response capability for probabilistically significant operating modes and initiating event categories (internal, external, flood, fire, seismic, etc.). Given a full scope 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 full scope level 2 PRA, surrogate information should be developed for unanalyzed areas, along the lines described in Section II.3.2.2. This requirement is necessary in order to show the safety functions performed by SSCs affected by the application.
- Causal models (determination of cause-effect relationships) should be developed to support quantification of basic event probability as a function of the application. This is necessary in order to relate the application to actual risk indices.

Documentation of inputs to the decisionmaking panel should be part of the process. The reviewer should verify the scope and depth of the information base, especially information supplied regarding modes and/or classes of initiators unanalyzed in the PRA.

Treatment of SSCs not Modeled in the PRA:

PRA's do not model all SSCs involved in performance of safety functions for various reasons. However, this should not imply that unmodeled SSCs are not important in terms of contributions to the plant risk. For example, 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 results will not reflect the SSC at all, it would be inappropriate to conclude that the programmatic activity is unimportant.

It is one of the tasks of the integrated decisionmaking panel to extrapolate from the PRA and other information sources to draw conclusions about SSCs not modeled in the PRA. This does not mean that the panel is 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 panel is justified in reasoning that unmodeled SSCs in that path are relied upon. If items were screened from the PRA, the panel should be aware of the screening process, in order to avoid violating the basis for the screening.

For SSCs not modeled in the PRA, the reviewer should verify that the decisionmaking panel has performed the following:

DRAFT FOR COMMENT

- 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 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. In cases where reduced commitments are proposed, adequate justification is provided for this reduction;
- the item does not currently receive sufficient programmatic attention, and may be subject to tighter controls.

The reviewer should verify that the safety significance of SSCs not modeled in the PRA (but affected by the proposed application) are appropriately characterized and justified.

Addressing limitations of the risk analysis:

Part of the integrated decisionmaking process is to overcome certain limitations of the PRA. However, this does not include substituting the analyst's judgment for essential PRA results. One of the reasons for developing PRA models is that the complexity of many facilities makes judgment difficult in many contexts.

Generally, if PRA highlights a plant vulnerability, this should be taken seriously. This result should not be discounted on the basis of judgment. If the analyst can show that the PRA representation of a vulnerability is invalid, then the PRA should be modified, and the licensee should work with the results of the revised PRA.

To address the issue of credit for unmodeled systems that would change a PRA

DRAFT FOR COMMENT

result, the preferred method is to alter the PRA to take the credit. The reviewer should be aware that 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 such as spatial interaction issues or operator interaction dependencies.

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 SSC. While it is possible to accept program reductions for SSCs that are explicitly shown to play no role in unanalyzed 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.

To address instances in which a PRA model exists but is considered misleading, caution is indicated. An example of this would be to down-classify SSCs (i.e., state that a high risk contributor is actually a low contributor) from a PRA result, based on panel judgment. It is not acceptable to place on the record both a PRA and a finding that clearly contradicts it. Although the panel is not expected 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. 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 integrated decisionmaking process is appropriate. Appropriate information was available, suitable issues were raised, the disposition of these issues was systematic and defensible, and the documentation of the findings is traceable and reviewable in principle, so that the basis for conclusions and recommendations is available for scrutiny and review.
- The evaluation of risk significance represents appropriate consideration of probabilistic information, traditional engineering evaluations, sensitivity studies, operational experience, engineering judgment, and current regulatory requirements.

DRAFT FOR COMMENT

- The technical information basis was adequate for the scope of the application. 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.
- The safety significance of components affected by the proposed application but not modeled in the PRA was evaluated in a systematic manner. This included a search of 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 process applied by the licensee to overcome limitations of PRA was appropriate. Where decisions were made that do not follow straightforwardly from the PRA, a technical basis was provided that shows how the PRA information and the supplementary information validly combine to support the finding. No findings contradict the PRA in a fundamental way.

DRAFT FOR COMMENT

Appendix C

CATEGORIZATION OF STRUCTURES, SYSTEMS, AND COMPONENTS WITH RESPECT TO SAFETY SIGNIFICANCE

For several of the proposed applications of the risk-informed regulation process one of the principal activities is the categorization of SSCs and human actions with respect to their safety-significance. The purpose of this Appendix is to discuss how to review approaches that may be used in this categorization process.

The first review consideration is the definition of safety-significance as applied to SSCs and human actions for a specific application. A related, but not identical concept, is that of risk significance. For example, an individual SSC can be identified as being risk-significant if it can be demonstrated that its failure or unavailability contributes significantly to the measures of risk, e.g., CDF and LERF. Safety-significance, on the other hand, can be thought of as being related to the role the SSC plays in the prevention of the occurrence of the undesired end state. Thus the position adopted in this SRP is that all the SSCs and human actions considered when constructing the PRA model (including those that do not necessarily appear in the final quantified model, either because they have been screened initially, assumed to be inherently reliable or have been truncated from the solution of the model) have the potential to be safety significant, since they play a role in preventing core damage.

In reviewing the categorization, it is important to recognize the purpose behind the categorization, which is, generally, to sort out the SSCs or human actions into two general groups: those for which some change is proposed; and those for which no change is proposed. It is the potential impact of the application on the particular SSCs and human actions and on the measures of risk which ultimately determines which of the SSCs and human actions should be regarded as safety-significant. Since different applications impact different SSCs and human actions, it is reasonable to expect that the categorization could be different for the different applications. Thus the question being addressed by the application is, for which groups of SSCs and human actions can the change be made such there will be no more than insignificant increase in the risk to the health and safety of the public. This impact on overall risk should be related back to the criteria for acceptable changes in the risk measures identified in draft guide DG-1061. It is those groups for which changes can be made that satisfy these criteria that can be regarded as low safety-significant in the context of the specific application. Thus, the most appropriate way to address the categorization is through a requantification of the risk measures. However, the feasibility of performing such risk quantification has been questioned for those applications for which a method for the evaluation of the impact of the change on SSC unavailability is not obviously available.

In the above case, an acceptable alternative to requantification of risk is to perform the categorization of the SSCs and human actions using an

DRAFT FOR COMMENT

integrated decisionmaking process (such as the use of an Expert Panel), based on the use of PRA importance measures as input. The issues that should be addressed by the reviewer for this approach are discussed in this appendix. Section C.1 discusses the technical issues associated with the use of PRA importance measures, and Section C.2 discusses the use of the importance measures by the decisionmaking panel.

C.1 Use of Importance Measures

a. Area of Review

In the implementation of the Maintenance Rule and in many industry guides for the risk-informed applications, the Fussell-Vesely Importance, Risk Reduction Worth, and Risk Achievement Worth are the most commonly identified measures in the relative risk ranking of SSCs. However, in the use of these importance measures for risk-informed applications, there are several issues that should be addressed. Most of the issues are related to technical problems which can be resolved by the use of sensitivity studies or by appropriate quantification techniques. These issues are discussed in detail in the sub-section below. In addition, there are two issues that the reviewer should insure have been addressed adequately, namely a) that risk rankings apply only to individual contributions and not to combinations or sets of contributors, and b) that risk rankings are not necessarily related to the risk changes which result from those contributor changes. When performed and interpreted correctly, component-level importance measures can provide valuable input to the integrated decisionmaking process.

b. Review Guidance and Procedures

Risk ranking results from a PRA can be affected by many factors, the most important being model assumptions and techniques (e.g., for modeling of human reliability or common cause failures), the data used, or the success criteria chosen. The reviewer should therefore perform an evaluation of the licensee PRA as part of the overall review process. Guidance for this review is provided in Appendix A.

In addition to the use of a PRA of appropriate quality for the application, the robustness of risk ranking results should also be demonstrated for conditions and parameters that might not be addressed in the base PRA. Therefore, when importance measures are used to group components or human actions as low safety-significant contributors, the information to be provided to the integrated decisionmaking process should include sensitivity studies and/or other evaluations to demonstrate the sensitivity of the importance results to the important PRA modeling techniques, assumptions, and data. Issues that should be considered and addressed are listed below.

Different risk metrics: The reviewer should ensure that risk in terms of both CDF and LERF is considered in the ranking process.

DRAFT FOR COMMENT

Completeness of risk model: The reviewer should ensure that, when determining safety significance contributions using an internal events PRA, external events and shutdown and low power initiators have also been considered either by PRA modeling or by the integrated decisionmaking process (as detailed in section C.2 and in Appendix B).

Sensitivity analysis for component data uncertainties: The sensitivity of component categorizations to uncertainties in the parameter values should have been addressed by the licensee. Reviewers should be satisfied that SSC categorization is not affected by data uncertainties.

Sensitivity analysis for common cause failures: CCFs are modeled in PRAs to account for dependent failures of redundant components within a system. As discussed in Appendix A, CCF probabilities can impact PRA results by enhancing or obscuring the importance of components. This should be addressed by the review. A component may be ranked as a high risk contributor mainly because of its contribution to CCFs, or a component may be ranked as a 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.

Consideration of multiple failure modes: PRA basic events represent specific failure events and failure modes of SSCs. The reviewer should determine that the safety significant categorization has been performed taking into account the combined effect of all associated basic PRA events, such as failure to start and failure to run, including indirect contributions through associated CCF event probabilities.

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 recovery actions were removed. The reviewer should ensure that the categorization has not been unduly impacted by the modeling of recovery actions.

Truncation limit: The reviewer should determine that the truncation limit has been set low enough so that the truncated set of minimal cutsets contain 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. Depending on the PRA level of detail (module level, component level, or piece-part level), this may translate into a truncation limit from $1\text{E-}12$ to $1\text{E-}8$ per

DRAFT FOR COMMENT

reactor year. In addition, the truncated set of minimal cutsets should be determined to contain the important application-specific contributors and their logical combinations.

Multiple component considerations: As discussed previously, Importance measures are typically evaluated on an individual SSC or human action basis. One potential concern raised by this is that single-event importance measures have the potential of dismissing all elements of a system or group despite the system or group having a high importance when taken as a whole. (Conversely, there may be grounds for screening out groups of SSCs, owing to the unimportance of the systems of which they are elements.) There are two potential approaches to addressing the multiple component issue. The first is to define suitable measures of system or group importance. The second is to choose appropriate criteria for categorization based on component-level importance measures. In both cases, it will be necessary for the licensee to demonstrate that the cumulative impact of the change has been adequately addressed.

While there are no widely-accepted definitions of system or group importance measures, it is likely that some licensees will develop new system or group measures. If any are proposed, the reviewer should make sure that the measures are capturing the impact of changes to the group in a logical way. As an example of the issues that arise consider the following. For front-line systems, one possibility would be to define a Fussell-Vesely type measure of system importance as the sum of the frequencies of sequences involving failure of that system, divided by the sum of all sequence frequencies. Such a measure would need to be interpreted carefully if the numerator included contributions from failures of that system due to support systems. Similarly, a Birnbaum-like measure could be defined by quantifying 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. However, again the support systems make the situation 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.

In the absence of appropriately defined group level importance measures, reliance should be made on the integrated decisionmaking process to make the appropriate determination (see section C.2).

Relationship of Importance Measures to risk changes: Importance measures do not directly relate to changes in risk associated with implementation of a set of changes proposed in an application. Instead, the risk impact is indirectly reflected in the choice of the value of the measure used to determine whether an SSC should be classified as being of high and low safety significance. This is a concern whether importances are evaluated at the component or at the group level. The PSA Applications Guide suggested values of Fussell-Vesely importance of .05 at the system level, and .005 at the component level for

DRAFT FOR COMMENT

example. However, the criteria for categorization into low and high significance should be related to the acceptance guidelines for changes in CDF and LERF. This implies that the criteria should be a function of the base case CDF and LERF rather than being fixed for all plants. Thus the reviewer should determine how the choice of criteria are related to, and conform with, the acceptance guidelines described in draft guide DG-1061. If component level criteria are used, they should be established taking into account that the allowable risk increase associated with the change should be based on simultaneous changes to all members of the category.

c. Evaluation Findings

The reviewer verifies that the information provided to the integrated decisionmaking process on the determination of risk importance of contributors for a specific application is robust in terms of model inputs and assumptions and "uncertainty" issues like common cause failure modeling and modeling of human reliability, and that the categorization addresses the effect of the on groups of components in a way that is compatible with the risk acceptance guidelines.

C.2 Role of Integrated Decisionmaking in Component Categorization

a. Areas of Review

While probabilistic importance analysis can provide valuable information on categorization, it should be supported and supplemented by an evaluation based on traditional engineering considerations. This will require using the qualitative insights obtained from the PRA, and the incorporation of the consideration of maintenance of defense-in-depth and the maintenance of sufficient safety margins. One important element of this integrated decisionmaking can be the use of an "expert panel". General review guidelines for the licensee integrated decisionmaking process are provided in Appendix B of this SRP.

b. Review Guidance and Procedures

Identification of functions, systems and components important to safety: The PRA can provide significant qualitative insights that emerge 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. However, the real importance of a system is a function of whether there are alternate, diverse systems that could fulfil the same function, those systems which are the only means of providing the function being more important than those for which there are viable alternatives. A system that supports an important front-line system could also be important. This does not mean that all such systems cannot be candidates for relaxation in current

DRAFT FOR COMMENT

requirements, it does mean that components in system trains credited in the PRA should be explicitly considered during the integrated decisionmaking process.

The reviewer, either by evaluation of licensee documentation or by independent verification, should:

- identify all systems that are relied upon in plant response to an initiating event, whether explicitly modeled in the PRA or not (e.g., HVAC, I&C associated with indications rather than control), and identify the function(s) they perform or support; and
- check to see whether failure of components screened out on the basis that they are elements of "unimportant" systems could affect a system that is relied upon in plant response to an initiating event.

The reviewer should then verify that at least some elements of each of the important systems as identified above are considered "safety 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 programmatic activities allocated to these elements are commensurate with that performance level. If a system is identified as being important but none of its elements is, then licensee justification should be reviewed in detail.

As an example 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 as a whole. The focus of the above guidance is that the redundant flowpaths, considered as a subsystem, and recognizing the function they perform, are important and deserve some attention, even though conventional importance measures would not highlight them. However, in the case of redundant systems, the solution need not always be 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 and a program that addresses common cause failure potential by monitoring component performance may provide the necessary protection against loss of the function while still allowing a decrease in some level of commitment on the individual members of the group.

Verification of low safety significance: As part of the evaluation of the qualitative risk-informed categorization, the integrated decisionmaking process and criteria used by the licensee should be reviewed.

In reviews of the licensee determination of low safety significance for SSCs or operator actions, the staff should verify that risk importance measures have been applied appropriately and that results of sensitivity studies have been taken into account. In addition, the reviewer should verify that the licensee has considered and has compensated for factors such as potential inadequate scope and level of detail of the PRA (see sections II.3.2.2 and

DRAFT FOR COMMENT

II.3.2.3). Finally, the reviewer should verify that, in categorizing an SSC or operator action as low safety significance, the licensee has considered the defense-in-depth philosophy and available safety margins. Review guidance on these topics is provided in Section II.3.1 of this SRP.

For SSCs not modeled in the PRA, the reviewer should verify that the following conditions are applicable for each SSC that has been proposed as a candidate for relaxation or removal of current requirements:

- the SSC is not a part of a system that acts as a barrier to fission product release during severe accidents
- the SSC does not perform a support function to a safety function or does not complement a safety function
- the SSC does not support operator actions credited in PRAs for either procedural or recovery actions
- the failure of the SSC will not result in the eventual occurrence of a PRA initiating event
- the failure of the SSC will not result in unintentional releases of radioactive material even in the absence of severe accident conditions

If any of the above conditions are applicable, or if SSC performance is difficult to quantify, the licensee 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 one or more of the following justifications (or similar) were provided by the licensee:

- a qualitative discussion and historical evidence why these failure modes may be unlikely to occur;
- a qualitative engineering discussion on how such failure modes could be detected in a timely fashion;
- a discussion on what other requirements may be useful to control such failure rate increases; and
- a qualitative engineering discussion on why relaxing the requirements may have minimum impact on the failure rate increase.

c. Evaluation Findings

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

DRAFT FOR COMMENT

- The categorization of the SSCs or human actions has adequately captured their significance to safety, and has been performed in such a way that the potential impact of the proposed application results in at most a small increase in the risk to the health and safety of the public. The input to the integrated decisionmaking process derived from Importance measures has been utilized taking into account the known limitations of importance calculations, and the results have been supplemented by appropriate qualitative considerations.
- The integrated decisionmaking process explicitly recognized systems invoked in plant response to initiating events, and ensured that components within 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.



UNITED STATES NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION

DRAFT FOR COMMENT

Standard Review Plan
For The Review Of
Risk-Informed Inservice Testing Applications

Draft SRP Chapter 3.9.7

Revision 2C

March 13, 1997

Contacts: D. C. Fischer (301) 415-2728
W. B. Hardin (301) 415-6561

DRAFT FOR COMMENT

Standard Review Plan

For The Review Of

Risk-Informed Inservice Testing Applications

FOREWORD

The NRC's Policy Statement on the use of probabilistic risk analysis (PRA) in nuclear regulatory activities encourages greater use of this analysis technique to improve safety decision making, reduce unnecessary burden and improve regulatory efficiency. A number of NRC staff and industry activities are in progress to consider approaches for expanding the scope of PRA applications in regulatory activities.

Several activities are ongoing which consider appropriate uses of PRA in support of the modification of individual plant's current licensing basis (CLB) and a number of pilot applications with proposed CLB changes are now under staff review.

This Standard Review Plan (SRP) chapter describes review procedures and acceptance guidelines for NRC staff reviews of proposed plant-specific, risk-informed changes to a licensee's inservice testing (IST) program. The review procedures contained in this SRP are consistent with the acceptable methods for implementing a risk-informed IST (RI-IST) program described in DG-1062 (reference 2). Licensees may propose RI-IST programs consistent with the guidance provided in DG-1062, propose an alternative approach for implementing a RI-IST program (which must be demonstrated to be consistent with the fundamental principles identified in Section II.A.9), or maintain their IST programs in accordance with the ASME Code as referenced in 10 CFR 50.55a.

It is the NRC staff's intention to initiate rulemaking as necessary to permit licensees to implement RI-IST programs, consistent with this SRP chapter, without having to get NRC approval of an alternative to the ASME Code requirements pursuant to 10 CFR 50.55a(a)(3). Until the completion of such rulemaking, the staff anticipates reviewing and approving each licensee's RI-IST program as an alternative to the current Code required IST program (e.g., including alternative test frequency, test methods, and program scope requirements). As such, the licensee's RI-IST program will be enforceable under 10 CFR 50.55a.

The current ASME Code inservice testing requirements, as endorsed in 10 CFR 50.55a, have been determined to provide reasonable assurance that public health and safety will be maintained. The individual ASME Code committees

DRAFT FOR COMMENT

concerned with inservice testing of pumps and valves continually review these testing strategies to develop improvements to the existing Code requirements. Changes to the ASME Code, either as new Code editions or Code Cases, are subject to review and approval by the NRC to ensure that the new testing requirements maintain an adequate level public health and safety. A risk-informed inservice testing program, if properly constructed, will also provide an acceptable level of quality and safety by evaluating and possibly improving the test effectiveness for the high safety significant components (as identified by the licensee's PRA and integrated decision making process) in conjunction with the relaxation of testing requirements (e.g., test frequency) for the low safety significant components.

DRAFT FOR COMMENT

Standard Review Plan

For The Review Of

Risk-Informed Inservice Testing Applications

TABLE OF CONTENTS

3.9.7 RISK-INFORMED INSERVICE TESTING OF PUMPS AND VALVES

| | <u>Page</u> |
|--|-------------|
| REVIEW RESPONSIBILITIES | 1 |
| I. DEFINE THE PROPOSED CHANGES TO THE IST PROGRAM . | 1 |
| II. AREA OF REVIEW | 2 |
| A. ENGINEERING EVALUATION | 2 |
| 1. Evaluation of Proposed Changes to the Current Licensing Basis . . | 2 |
| 2. IST Program Scope | 3 |
| 3. IST Program Changes | 4 |
| 4. Relief Requests and Technical Specification Amendments | 4 |
| 5. Quality of the PRA for IST Application | 4 |
| 6. Modeling of the Effects of IST on PRA Basic Events | 4 |
| 7. Categorization of Components | 4 |
| 8. Other Technical Issues | 5 |
| a. Initiating Events | 5 |
| b. Dependencies and Common Cause Failures | 5 |
| c. Uncertainty and Sensitivity Analyses | 6 |
| d. Human Reliability Analyses | 6 |
| e. Use of Plant-Specific Data | 6 |
| 9. Evaluating the Overall Effect of Proposed Changes on Plant Risk . | 7 |
| 10. Integrated Decision Making | 7 |
| B. IMPLEMENTATION, PERFORMANCE MONITORING, AND CORRECTIVE ACTION | 9 |
| 1. Program Implementation | 9 |
| 2. Performance Monitoring of IST Equipment | 9 |

DRAFT FOR COMMENT

| | |
|---|-----------|
| 3. Feedback and Corrective Action Program | 9 |
| 4. Periodic Reassessment | 9 |
| 5. Formal Interactions With the NRC | 10 |
| III. ACCEPTANCE GUIDELINES | 10 |
| A. ENGINEERING EVALUATION | 10 |
| 1. Evaluation of Proposed Changes to the Current Licensing Basis . . | 10 |
| 2. IST Program Scope | 10 |
| 3. IST Program Changes | 11 |
| 4. Relief Requests and Technical Specification Amendments | 12 |
| 5. Quality of the PRA for IST Application | 12 |
| 6. Modeling of the Effects of IST on PRA Basic Events | 13 |
| 7. Categorization of Components | 13 |
| 8. Other Technical Issues | 13 |
| a. Initiating Events | 13 |
| b. Dependencies and Common Cause Failures | 14 |
| c. Uncertainty and Sensitivity Analyses | 14 |
| d. Human Reliability Analyses | 14 |
| e. Use of Plant-Specific Data | 15 |
| 9. Evaluating the Overall Effect of Proposed Changes on Plant Risk . | 15 |
| 10. Integrated Decision Making | 15 |
| B. IMPLEMENTATION, PERFORMANCE MONITORING, AND CORRECTIVE ACTION | 17 |
| 1. Program Implementation | 17 |
| 2. Performance Monitoring of IST Equipment | 18 |
| 3. Feedback and Corrective Action Program | 19 |
| 4. Periodic Reassessment | 19 |
| 5. Formal Interactions With the NRC | 20 |
| IV. REVIEW PROCEDURES | 21 |
| A. REVIEW OF THE LICENSEE'S ENGINEERING EVALUATION | 21 |
| 1. Evaluation of Proposed Changes to the Current Licensing Basis . . | 21 |
| 2. IST Program Scope | 21 |
| 3. IST Program Changes | 21 |
| 4. Relief Requests and Technical Specification Amendments | 23 |
| 5. Quality of the PRA for IST Application | 24 |
| 6. Modeling of the Effects of IST on PRA Basic Events | 25 |
| 7. Categorization of Components | 26 |
| 8. Other Technical Issues | 26 |
| a. Initiating Events | 26 |
| b. Dependencies and Common Cause Failures | 26 |
| c. Uncertainty and Sensitivity Analyses | 27 |

DRAFT FOR COMMENT

| | | |
|-------|--|----|
| d. | Human Reliability Analyses | 27 |
| e. | Use of Plant-Specific Data | 28 |
| 9. | Evaluating the Overall Effect of Proposed Changes on Plant Risk | 28 |
| 10. | Integrated Decision Making | 28 |
| B. | REVIEW IMPLEMENTATION, PERFORMANCE MONITORING, AND CORRECTIVE ACTION | 29 |
| 1. | Program Implementation | 29 |
| 2. | Performance Monitoring of IST Equipment | 31 |
| 3. | Feedback and Corrective Action Program | 31 |
| 4. | Periodic Reassessment | 31 |
| 5. | Formal Interactions With the NRC | 32 |
| V. | EVALUATION FINDINGS | 32 |
| A. | ENGINEERING EVALUATION | 33 |
| 1. | Evaluation of Proposed Changes to the Current Licensing Basis | 33 |
| 2. | IST Program Scope | 33 |
| 3. | IST Program Changes | 33 |
| 4. | Relief Requests and Technical Specification Amendments | 35 |
| 5. | Quality of the PRA for IST Application | 35 |
| 6. | Modeling of the Effects of IST on PRA Basic Events | 36 |
| 7. | Categorization of Components | 36 |
| 8. | Other Technical Issues | 37 |
| a. | Initiating Events | 37 |
| b. | Dependencies and Common Cause Failures | 37 |
| c. | Uncertainty and Sensitivity Analyses | 37 |
| d. | Human Reliability Analyses | 37 |
| e. | Use of Plant-Specific Data | 38 |
| 9. | Evaluating the Overall Effect of Proposed Changes on Plant Risk | 38 |
| 10. | Integrated Decision Making | 39 |
| B. | IMPLEMENTATION, PERFORMANCE MONITORING, AND CORRECTIVE ACTION | 39 |
| 1. | Program Implementation | 39 |
| 2. | Performance Monitoring of IST Equipment | 40 |
| 3. | Feedback and Corrective Action Program | 40 |
| 4. | Periodic Reassessment | 41 |
| 5. | Formal Interactions With the NRC | 41 |
| VI. | RISK-INFORMED IST PROGRAM DOCUMENTATION | 42 |
| VII. | IMPLEMENTATION | 42 |
| VIII. | REFERENCES | 42 |

DRAFT FOR COMMENT

DRAFT FOR COMMENT

Standard Review Plan

For The Review Of

Risk-Informed Inservice Testing Applications

3.9.7 RISK-INFORMED INSERVICE TESTING

REVIEW RESPONSIBILITIES

Primary - Mechanical Engineering Branch (EMEB)

Secondary - Probabilistic Safety Assessment Branch (SPSB)

I. DEFINE THE PROPOSED CHANGES TO THE IST PROGRAM

The licensee's risk-informed inservice testing (RI-IST) submittal should have defined the proposed changes to the IST program in general terms. The licensee should have confirmed that the plant is designed and operated in accordance with the current licensing basis (CLB)¹ and that the PRA used in support of their RI-IST program submittal reflects the actual plant. The licensee should have identified the particular components that would be affected by the proposed changes in IST strategy. This should include all of the components currently in the licensee's IST program as well as any other

¹ This regulatory guide adopts the 10 CFR Part 54 definition of current licensing basis. That is, "Current Licensing Basis (CLB) is the set of NRC requirements applicable to a specific plant and a licensee's written commitments for ensuring compliance with and operation with in applicable NRC requirements and the plant-specific design basis (including all modifications and additions to such commitments over the life of the license) that are docketed and in effect. The CLB includes the NRC regulations contained in 10 CFR Parts 2, 19, 20, 21, 26, 30, 40, 51, 54, 55, 70, 72, 73, 100 and appendices thereto; orders; license conditions; exemptions; and technical specifications. It also includes the plant-specific design-basis information defined in 10 CFR 50.2 as documented in the most recent final safety analysis report (FSAR) as required by 10 CFR 50.71 and the licensee's commitments remaining in effect that were made in docketed licensing correspondence such as licensee responses to NRC bulletins, generic letters, and enforcement actions, as well as licensee commitments documented in NRC safety evaluations or licensee event reports."

DRAFT FOR COMMENT

components that the licensee's integrated decision making process categorized as being highly safety significant. The method used by the licensee to categorize components should be described. There should also be a detailed description of how the proposed RI-IST program affects the CLB of the plant and why these proposed changes are acceptable. If exemptions from specific regulations, technical specification amendments, or relief requests are required to implement the licensee's proposed RI-IST program, the appropriate requests should accompany the licensee's submittal. Specific revisions to testing schedules and methods should be described as well as implementation plans and schedules.

The licensee should also have described the proposed IST program change in terms of how it meets the objectives of the Commission's PRA Policy Statement, including enhanced decision making, more efficient use of resources, and reduction of unnecessary burden. The description may consider benefits from the CLB change such as reduced fiscal and personnel resources and radiation exposure, as well as improvements in reactor safety.

The reviewer should familiarize herself or himself with the licensee's entire submittal before initiating the detailed review described in the following sections. In short, the reviewer should first develop an understanding of the proposed change in terms of:

- the particular components that would be affected by the proposed changes in IST strategy,
- the plant systems involved with the proposed changes in IST strategy,
- the change in testing strategy (i.e., test frequency and methods) proposed for each component or group of components,
- its affect on the current licensing basis, and
- its overall effect on plant risk.

Section 6 of reference 2 contains a more detailed description of the documentation that should have been submitted by the licensee in conjunction with its proposed RI-IST program.

II. AREA OF REVIEW

A. ENGINEERING EVALUATION

1. Evaluation of Proposed Changes to the Current Licensing Basis

After the licensee determined which components are candidates for having their inservice test requirements relaxed and which components should be subjected

DRAFT FOR COMMENT

to more focused inservice tests, the licensee should have conducted an engineering evaluation of proposed changes to the IST program. The purpose of this engineering evaluation is to determine the acceptability of the proposed IST program changes in light of the current licensing basis of the plant and risk impact of the changes. In particular, the status of license commitments that would be changed as a result of the proposed RI-IST program should have been clarified explicitly and formally. Either commitments were not affected by the proposed changes, or the alterations in commitment status were identified, described, and revised commitments were made.

2. IST Program Scope

In developing RI-IST programs, licensees will likely identify structures, systems, and components (SSCs) with high risk significance which are not currently subject to traditional Code requirements or subject to a level of regulation which is commensurate with their risk significance. It is expected that licensees will propose RI-IST programs that will subject these SSCs to the appropriate level of regulation, consistent with the risk significance of the SSC. Specifically, licensee's RI-IST program scope should include, in addition to components in the current Code prescribed IST program (e.g., components required to perform a specific function in shutting down a reactor to a cold shutdown condition, in maintaining the cold shutdown condition, or in mitigating the consequences of an accident), those ASME Code Class 1, 2, & 3 and non-Code components that the licensee's integrated decision-making process categorized as highly safety significant and determined to be appropriate candidates for IST.

The staff's basis for reaching its conclusion that the licensee's proposed RI-IST program "provides an acceptable level of quality and safety" will be predicated, in part, on the licensee's use of PRA to identify the appropriate scope of components that should be included in a RI-IST program as well as to evaluate test requirements (i.e., test methods and frequency) to ensure the validity of PRA assumptions. In other words, if the PRA is to be used as the basis for categorizing components and for evaluating the acceptability of the overall change in plant risk associated with the proposed RI-IST program (e.g., ΔCDF , $\Delta LERF$) then the PRA assumptions relative to component reliability and availability must be preserved. Consequently, for IST components within the scope of the licensee's proposed RI-IST program, we would expect the licensee to examine the test strategies currently in place and, where appropriate, modify the test strategy (See Section III.A.3).

To preserve the PRA assumptions which form the basis for the acceptability of the IST program changes, certain non-Code components may need to be included in the RI-IST program. The justification for inclusion of non-code components into the IST program can be derived from the role these components play in justifying the acceptability of changes to the IST program for components currently within the code. PRA systematically takes credits for non-code structures, systems, and components (SSCs) as: 1) providing support to, or 2) alternatives to, and 3) back-ups for SSCs within the current code. Thus, the

DRAFT FOR COMMENT

relaxation of requirements for safety-related SSCs depends upon the proper operation and reliability attributed to high-safety-significant yet non-code SSCs.

3. IST Program Changes

The licensee's submittal should describe the considerations (e.g., component performance, service condition, risk significance) that went into establishing the proposed RI-IST frequencies and methods.

4. Relief Requests and Technical Specification Amendments

While implementation of the licensee's overall RI-IST program may be authorized by a change to the regulations or via NRC authorizing an alternative pursuant to 10 CFR 50.55(a)(3), specific details of the licensee's RI-IST program may require exemptions from other regulations, technical specification changes, or require relief from provisions of NRC approved Codes or Code cases. The license should have included in their RI-IST program submittal the necessary exemption requests, technical specification amendment requests, relief requests, and relief requests necessary to implement their RI-IST program (See Section III.A.4).

5. Quality of the PRA for IST Application

Since the quantitative results of the PRA are to play a major and direct role in decision-making, there is a need to ensure that they are derived from "quality" analyses. Review guidance in quality issues for the licensee's baseline PRA is provided in the general regulatory guide for risk informed decision making (Reg Guide DG-1061) and in the general SRP for risk informed regulation (Chapter 19 of the SRP). The required scope and level of detail of the PRA are also discussed in the general Reg Guide and SRP. The review of IST-specific issues, i.e., those pertaining to areas most directly related to IST, are discussed in this IST SRP.

6. Modeling of the Effects of IST on PRA Basic Events

One of the requirements for the acceptability of a risk informed IST program is a quantitative demonstration by use of a PRA of sufficient quality that changes to plant risk caused by the proposed extension in testing intervals or changes in test methods for selected components are small or are reductions and should not cause the NRC Safety Goals to be exceeded (See reference 1). In order to establish this demonstration, it is necessary that the PRA include models which appropriately account for the change in reliability of the components as a function of testing interval. For many purposes, it is also desirable to model the effects of enhanced testing methods. Components not modeled in the PRA should be evaluated and categorized with appropriate basis.

7. Categorization of Components

DRAFT FOR COMMENT

The identification of components as potential candidates for changes in IST intervals or test methods can be done in many ways. Component categorization using PRA importance measures to classify structures, systems, and components (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 licensee's integrated decision-making process (e.g., expert panel) to help determine the safety significance of the IST components.

In addition to the determination of risk importance contribution for input to the licensee's integrated decision-making process, the determination of potential risk contribution from SSCs by PRA importance determination can be useful for the following reasons:

- When performed with a series of sensitivity evaluations, it can identify potential risk outliers by identifying components which could dominate risk for various plant configurations and operational modes, PRA model assumptions, and data and model uncertainties.
- Importance categorization can provide a useful means to identify improvements to current IST practices during the risk-informed application process by identifying components that are high risk contributors which may benefit from more frequent tests or enhanced testing methods.

8. Other Technical Issues

a. Initiating Events

While completely new initiating events are not expected from proposed changes to IST programs, it is necessary to review whether initiating events previously screened out in the PRA, on grounds of low frequency, might now be above the screening threshold as a result of an IST program change. Examples would be events that are (a) relatively infrequent to begin with, (b) mitigated satisfactorily by closure of an isolation valve, and (c) not analyzed because of a combination of low frequency of event "AND-ed" with a low probability of valve failure. If such events increased in frequency as a result of an IST program change, then the scope of consideration would need to change to reflect this.

b. Dependencies and Common Cause Failures (CCFs)

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

A change in IST has the potential of affecting the CCF probabilities since similar test methods and frequencies are being proposed for pumps or valves as

DRAFT FOR COMMENT

a group. For these 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 in IST frequencies and methods, there should be assurance that the CCF contribution will not become so significant that it could affect satisfying the acceptance criteria (See reference 1).

c. Uncertainty and Sensitivity Analyses

This issue consists of two parts. The first part deals with uncertainties in the baseline PRA that is used as the basis for the IST risk evaluation. A discussion for the need and criteria for an evaluation of uncertainties in the base PRA is provided in the general Reg Guide and SRP.

The second part of this issue is the matter of uncertainties in the estimates of the change in risk resulting from implementation of the risk informed IST program. If the licensee provides a best estimate indication of the change in risk, then an estimate of uncertainties is necessary in order to make a rational decision on the acceptability of the change. On the other hand, if the licensee provides an upper bound estimate of the change in risk based on a demonstrably conservative analysis, then an uncertainty analysis is not required.

d. Human Reliability Analysis

The results of a PRA, and therefore the decisions that are influenced by it, can be 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, in the IST area, 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 a test interval 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 an appropriate measure to support justification of a relaxation. Consistent with maintenance of defense in depth, operator action should not be the sole basis for determining that a testing interval can be extended.

e. Use of Plant-Specific Data

In selecting appropriate failure rate data to use in the risk informed IST program, 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,

DRAFT FOR COMMENT

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. Since several generic data bases are available, and they do not always agree, a further issue is which of these is most appropriate. Sections III.A.8.e and IV.A.8.e provides guidance.

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. Poor performance may arise because of inherent characteristics of one member of would otherwise be considered a uniform population. This would result in a higher than expected failure rate for the population and lead to less relaxation than might be anticipated. Of more concern is poor performance of components that arise because they are operating in a more demanding environment for example. If, for reasons of expediency, these components are grouped together with others for which the operating conditions are more favorable, then their failure rates could become artificially lowered, and, if requirements are relaxed based on the group failure rate, this could lead to a significant probability of experiencing an inservice failure of the poor performers.

9. Evaluating the Overall Effect of Proposed Changes on Plant Risk

The acceptance of risk-informed IST changes should depend on how the proposed changes affects the CLB in light of the following key principles:

- a. The proposed change meets the current regulations. [This principle applies unless the proposed change is explicitly related to a requested exemption or rule change.]
- b. The defense in depth philosophy is maintained.
- c. Sufficient safety margins are maintained.
- d. Proposed increases in risk, and their cumulative effect, are small and do not cause the NRC Safety Goals to be exceeded.
- e. Performance-based implementation and monitoring strategies are proposed that address uncertainties in analysis models and data and provide for timely feedback and corrective action.

10. Integrated Decision Making

The reviewer should evaluate the acceptability of the licensee's proposed RI-IST program using the proposed procedures outlined in Section IV of this SRP and the proposed acceptance guidelines specified Section III of this SRP. Each of the key principles specified in Section II.A.9 above should have been addressed in the licensee's submittal. In implementing these principles, the

DRAFT FOR COMMENT

reviewer should ensure that:

- All safety impacts of the proposed changes were evaluated on a component-specific basis as well as in an integrated manner as part of an overall risk management approach in which the licensee uses risk analysis to improve operational and engineering decisions broadly and not just to eliminate requirements that the licensee sees as undesirable. The approach used to identify changes in requirements should be used to identify areas where requirements should be increased as well as where they could be reduced.
- The acceptability of proposed changes should be evaluated by the licensee in an integrated fashion that ensures that all principles are met.²
- Core damage frequency (CDF) and large early release frequency (LERF) can be used as suitable metrics for making risk-informed regulatory decisions.
- Increases in estimated CDF and LERF resulting from proposed CLB changes will be limited to small increments.
- The scope and quality of the engineering analyses (including traditional and probabilistic analyses) conducted to justify the proposed CLB change should be appropriate for the nature and scope of the changes proposed and should be based on the as-built and as-operated and maintained plant.
- Appropriate consideration of uncertainty is given in analyses and interpretation of findings.
- The plant-specific PRA supporting decisions has been subjected to quality controls such as an independent peer review.
- Data, methods, and assessment criteria used to support the proposed IST program changes (e.g., those used by the licensee's expert panel) must be available for public review.

Acceptability of the proposed change should be determined using an integrated decision making process that addresses three major areas: (1) an evaluation of the proposed change in light of the plant's current licensing basis, (2) an evaluation of the proposed change relative to the key principles and the

² One important element of integrated decision making can be the use of an "expert panel." Such a panel is not a necessary component of risk-informed decision making; but when it is used, the key principles and associated decision criteria presented in this regulatory guide still apply and must be shown to have been met or to be irrelevant to the issue at hand.

DRAFT FOR COMMENT

acceptance criteria, and (3) the proposed plans for implementation, performance monitoring, and corrective action.

B. IMPLEMENTATION, PERFORMANCE MONITORING, AND CORRECTIVE ACTION

1. Program Implementation

The licensee should have an implementation plan and schedule for testing all high and low safety significant components identified in their program. Prior to the staff's approval of a RI-IST program, the NRC should review licensee's implementation plan and schedule. This plan should include test strategies (i.e., frequencies and methods) for high and low safety significant components that are within the scope of the licensee's RI-IST program, including components identified as high safety significant components that are not currently in the IST program. The composition of the component groupings (i.e., components of the same type, size, manufacturer, model, and that experience the same service conditions) should be identified. Components whose test interval is to be extended via staggering should be identified along with their staggered frequency over the test interval. Components should also be identified that are to have their test frequency extended using some other step-wise approach. The final test interval of these components should also be included in the submittal. [Section III.B.1 describes an acceptable method for extending test intervals in greater detail.]

2. Performance Monitoring of IST Equipment

Performance monitoring of IST equipment refers to the monitoring of test data for equipment that has been placed on an revised test strategy (e.g., extended test interval). The purpose of the performance monitoring is to help confirm that the failure rates assumed for this equipment remain valid, and that no unexpected failure mechanisms which are related to revised test strategy become important enough to alter the failure rate assumed in the evaluation models. Two important aspects of performance monitoring are whether the test frequency is sufficient to provide meaningful data, and whether the testing methods, procedures, and analysis provide assurance that performance degradation is detected. Component failure rates cannot be allowed to rise to unacceptable levels before detection and corrective action takes place.

3. Feedback and Corrective Action Program

A performance-based corrective action program should be a part of the licensee's proposed implementation and monitoring plan.

4. Periodic Reassessment

The reviewer should evaluate the licensee's RI-IST program to ensure that it contains explicit provisions whereby the overall program is periodically evaluated and component performance data gets fed back into both the component

DRAFT FOR COMMENT

grouping and component test strategy determination (i.e., test frequency and methods) process, and that changes will be made as appropriate. Reassessments should be performed at a frequency consistent with the availability of new data from the monitoring programs. This periodic reassessment should not be confused with the 120-month program updates required by 10 CFR 50.55a(f)(4)(ii) whereby the licensee's IST program must comply with later versions of the ASME Code that have been endorsed by the NRC.

5. Formal Interactions With the NRC

The reviewer should evaluate the licensee's proposed risk-informed IST program to determine if it appropriately describes the types of changes that can be made without prior NRC approval and the types of changes that require NRC approval prior to implementation (See Section III.A.1 and III.B.5).

III. ACCEPTANCE GUIDELINES

A. ENGINEERING EVALUATION

1. Evaluation of Proposed Changes to the Current Licensing Basis

The acceptance guidelines for evaluating proposed changes to the current licensing basis are contained in licensing basis documents as well as in other regulatory documents (e.g., regulations, regulatory guides, standard review plans, branch technical positions). The rules governing such changes are described in 10 CFR 50.59, 50.90, 50.109, and other regulations. Each proposed change must be evaluated on a case-by-case basis for acceptability. On a component-specific basis, the licensee should identify each instance where the proposed IST program change will affect the CLB of the plant and document the basis for the acceptability of the proposed change by explicitly addressing each of the key safety principles.

A broad evaluation of proposed changes to the CLB of the plant is appropriate because proposed IST program changes could affect requirements or commitments that are not explicitly described in the licensee's safety analysis report. Furthermore, staff approval of the design, operation, and maintenance of SSC at the facility may have been granted in terms other than probability, consequences, or margin of safety. Therefore, it may be more appropriate to evaluate proposed IST program changes against other more explicit criteria (e.g., design basis criteria used in either the licensing process or to determine the acceptability of SSC design, operation, and maintenance).

2. IST Program Scope

In order to be acceptable, the RI-IST program scope should include, in addition to components in the current Code prescribed program, any other components (e.g., pumps, valves, or snubbers) categorized as highly safety significant that were so identified as part of the PRA or licensee's integrated decision-making process (e.g., expert panel).

DRAFT FOR COMMENT

3. IST Program Changes

a. General

The licensee's RI-IST program should reevaluate the testing frequency (and methods as applicable) for high safety significant components that were the subject of a deferred test justification, an approved relief request, or an NRC authorized alternative test. The licensee should resubmit relief requests and proposed alternatives, along with risk-related insights, for NRC staff review and approval (see Section 4.1.4 of reference 2).

In establishing the test interval for low safety significant components, the licensee should consider component design, service condition, and performance as well as risk insights. The proposed test interval should be supported by both generic and plant-specific failure rate data and the test interval should be significantly less than the expected time to failure of the component in question (e.g., an order of magnitude less). Alternatively, the licensee could ensure that adequate component capability (i.e., margin) exists, above that required during design basis conditions, such that component operating characteristics over time do not result in reaching a point of insufficient margin before the next scheduled test activity. The inservice test interval should generally not be extended beyond once every 5 years or 3 refueling outages (whichever is longer) without specific compelling documented justification.

IST components (i.e. with the exception of check valves) should, at a minimum, be exercised or operated (i.e., via testing of other components in the system, routine maintenance, normal plant operations, etc.) at least once every refueling cycle. If practical, more frequent exercising should be considered for components in any of the following categories:

- a) Components with high safety significance;
- b) Components in adverse or harsh environmental conditions; or
- c) Components with any abnormal characteristics (operational, design, or maintenance conditions).

b. Changes to Test Interval (Only)

A RI-IST program that proposes to only adjust IST intervals should have provisions to:

- a) identify components whose test interval should be decreased as well as components whose test interval might be extended.
- b) assess the effectiveness of the current IST program in determining the ability of the component to carry out its intended function. Test intervals should only be extended for components that are tested using methods that have the capability to detect component degradation associated with the important failure modes and causes identified in the

DRAFT FOR COMMENT

plant's PRA.

If the licensee chooses the alternative described in reference 2 for implementing a RI-IST program, the licensee should make a commitment to adopt enhanced test strategies as described in risk-based IST Code cases developed by ASME as endorsed by the NRC or obtain staff authorization for an alternative test strategy.

c. Changes to Test Interval and Methods

A RI-IST program that adjusts IST intervals as well as IST methods is acceptable if it identifies components whose test strategy should be more focused as well as components whose test strategy might be relaxed.

4. Relief Requests and Technical Specification Amendments

The licensee should address the following issues:

- For low safety significant components, are there any component test methods that are not in accordance with the Code requirements or any NRC guidance? If so, relief is required for these test methods.
- For high safety significant components, are there any component test methods that are not in accordance with the Code requirements or any NRC guidance? If so, relief is required for these test methods.
- For high safety significant components, are there any component test frequencies that are not in accordance with the Code requirements or any NRC guidance? If so, relief is required for these test frequencies.
- For any components, are there changes in technical specification requirements? If so, the licensee is required to submit and have approval of a technical specification amendment prior to implementing the RI-IST program. Similarly, if a proposed IST program change requires a change to the updated Final Safety Analysis Report (USAR) change, the licensee should have performed an evaluation pursuant to 10 CFR 50.59.

5. Quality of the PRA for IST Application

In order to be acceptable for application to IST, the PRA models must reflect the dependence of core damage frequency (CDF) and large early release frequency (LERF) on basic events whose probabilities are affected by IST. This means that IST-related events and events that are logically in parallel with IST events must be quantified properly.

Modeling of IST events should:

- satisfactorily reflect dependence of basic event probability on fault

DRAFT FOR COMMENT

exposure time,

- consider effects of staggering of tests,
- use defensible failure rate parameters (λ), and if better-than-generic λ 's are used, special justification may be warranted,
- consider the effect on λ of aging, environmental stresses, and frequency of testing (either as part of the PRA, or as part of the licensee's integrated decision making process), and

In addition, common cause failure (CCF) modeling of failures potentially addressed by IST must be performed.

6. Modeling of the Effects of IST on PRA Basic Events

The PRA should include a model which can provide an appropriate measure of the change in risk as a result of extending the test interval on selected components. This requires that the model directly addresses the change in component availability as a function of test interval. The model must include:

- an explicit quantitative consideration of the degradation of the component failure rate as a function of time, supported by appropriate data and analysis,

OR

- arguments need to be presented which convincingly support the conclusion that no significant degradation will occur,

7. Categorization of Components

When using risk importance measures to identify components that are low risk contributors, potential limitations of these measures have to be addressed. Therefore, information to be provided to the licensee's integrated decision-making process (e.g., expert panel) must include sensitivity studies and/or other evaluations to demonstrate the insensitivity 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 include the following: truncation limit, different risk metrics, component failure modes, different maintenance states and plant configurations, multiple component considerations, defense in depth, binning criteria, and analysis of uncertainties (including sensitivity studies to component data uncertainties, common cause failures, and recovery actions).

8. Other Technical Issues

a. Initiating Events

DRAFT FOR COMMENT

Other than for IST interval extensions argued on the basis of IST-induced risk, the acceptance guideline in this area is that there should be positive evidence that the licensee process considered the effect of the IST program on initiating event frequency.

In the area of IST-induced risk, licensees are encouraged, to analyze the potential for adverse effects due to the tests themselves, and to look for ways to reduce these effects, either through changes in interval or changes in test protocols. If licensees advance the argument that there are significant adverse effects associated with testing as a reason for reducing or eliminating test frequency, then it will be necessary to review

- the causal model relating IST activity to the occurrence of an initiating event,
- the probability of core damage conditional on this event,
- the causal model relating reduction of IST or change in protocol to the subsequent behavior of the IST component.

Acceptance criteria for these causal models are the same as for causal models of IST basic events, and the acceptance criterion for core damage probability is covered by acceptance criteria for general PRA issues presented in the general SFP.

b. Dependencies and Common Cause Failures

Common cause failure (CCF) modeling of failures potentially addressed by IST should be performed. This includes the modeling of CCF groups of similar components that are mutually redundant and all being relaxed.

To reduce fault exposure times for potential common cause failures, staggered testing should be implemented as part of the RI-IST change process.

c. Uncertainty and Sensitivity Analyses

The criteria for the analysis of uncertainties in the comparison to acceptance guidelines is provided in the Regulatory Guide DG-1061 (reference 1).

d. Human Reliability Analysis

Justification of IST relaxations 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). However, credit may be taken for proceduralized implementation of alternative success strategies.

For each human action that compensates for a basic event probability increasing as a result of IST relaxation, there should be an explicit licensee commitment to ensure performance of the function at the level credited in the

DRAFT FOR COMMENT

quantification. Excessively low human failure probabilities (less than $1E-3$) cannot be accepted unless there is supporting analyses that justifies the use of the low human failure probability and there are adequate training programs, personnel practices, staff policies, etc. to ensure continued staff performance at this level.

e. Use of Plant-Specific Data

The acceptance guidelines for this issue are as follows:

- 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. For those licensees who propose to use plant specific data only, the data used should be consistent with the generally accepted values in other PRAs for CCFs and initiating event frequencies, or any significant deviations should be justified.
- As part of the performance monitoring, there should be an evaluation to determine if components that have experienced repeated failures 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 the testing strategy (interval and methods) would be considered adequate to support the performance credited of them in the risk analysis.

9. Evaluating the Overall Effect of Proposed Changes on Plant Risk

The general Regulatory Guide on Risk-Informed Decision Making (DG-1061) provides guidance for the acceptance of RI-IST changes and consideration in context with other RI initiatives.

10. Integrated Decision Making

The licensee's proposed RI-IST program should be supported by an engineering evaluation (reviewed in accordance with RI-IST SRP section IV.A). It is expected that the categorization developed by the PRA process and the traditional engineering approach will be considered by the licensee's integrated decision-making process (e.g., expert panel) to categorize components and in making decisions regarding each component's test strategy. The licensee's RI-IST program submittal should meet the acceptance guidelines contained in Section III. A.1 through 8 or justify why an alternative approach is acceptable.

Defense in depth has traditionally been applied in reactor design and operation to provide multiple means to accomplish safety functions and prevent the release of radioactive material. It has been and continues to be an effective way to account for uncertainties in equipment and human performance.

DRAFT FOR COMMENT

In some cases risk analysis can help quantify the range of uncertainty; however, there will likely remain areas of large uncertainty or areas not covered by the risk analysis. Where a comprehensive risk analysis can be done, it can be used to help determine the appropriate extent of defense in depth (e.g., balance among core damage prevention, containment failure, and consequence mitigation) to ensure protection of public health and safety. Where a comprehensive risk analysis is not or cannot be done, traditional defense in depth considerations should be used or maintained to account for uncertainties. Proposed RI-IST programs should be assessed to ensure that the defense in depth is maintained. Defense in depth is preserved if, for example:

- a reasonable balance is maintained between prevention of core damage, prevention of containment failure, and consequence mitigation;
- there is not an over-reliance on programmatic activities to compensate for weaknesses in plant design;
- system redundancy, independence, and diversity are maintained commensurate with the expected frequency and consequences of challenges to the system;
- defenses against potential common cause failures are maintained and the introduction of new common cause failure mechanisms are avoided;
- independence of barriers is not degraded
- defenses against human errors are maintained

Sufficient safety margins are maintained if, for example:

- ASME codes and standards or alternatives approved for use by the NRC are met;
- safety analysis acceptance criteria in the current licensing basis (e.g., USAR, supporting analyses) are met, or proposed revisions provide sufficient margin to account for analysis and data uncertainties;

Defense in depth and safety margin may be evaluated, as feasible, using risk techniques (PRA) provided Code-required margins are preserved.

Other acceptance guidelines may be proposed by the licensee. However, alternative guidelines would require more detailed consideration by the reviewer on a case by case basis.

After the components have been categorized, RI-IST program implementation, performance monitoring, and corrective action (Section III.B) acceptance guidelines should be satisfied and the overall effect of the proposed changes should be acceptable (ref. Section III.A.9) before the reviewer concludes that the proposed RI-IST program provides "an acceptable level of quality and

DRAFT FOR COMMENT

safety" [ref. 10 CFR 50.55a (a)(3)(i)].

If the licensee's proposed RI-IST program is unacceptable based on either traditional engineering analyses or the probabilistic analyses, the reviewer should deny the licensee's proposed RI-IST program.

In evaluating the overall effect of the proposed RI-IST program, the licensee should specifically evaluate the effect of the proposed relaxations of requirements (e.g., test interval extensions) for components considered singly and when grouped together. Where these relaxations are offset by alternative measures (e.g., additional monitoring, different tests, procedures, training), the licensee should identify, and quantify to the extent practicable, the effects of these alternative measures. Similarly, if there are benefits associated with proposed relaxations (e.g., reduction in initiating event frequency, reduction in system misalignment, reduction in radiation exposure), the licensee should identify, and quantify to the extent practicable, the effects of these benefits. As a general rule, the alternative measures and benefits should be directly linked to the systems or components associated with proposed relaxations. On a case by case basis, the staff may assess the licensee's proposed improvements made to the test strategy for a group of components against proposed relaxations in test requirements for another group of components in assessing the overall acceptability of a proposed RI-IST program. For example, the risk increase associated with relaxation of requirements for a group of low safety significant components may be deemed acceptable in light of improvements made to a group of more high safety significant components, even if all of the factors contributing to the overall change in risk are not quantified. However, the vulnerability associated with the relaxation of requirements for the low safety significant components must be acceptably low (See DG-1061 criteria). The licensee's integrated decision-making process should have explicitly considered all such situations. The factors considered by the licensee's integrated decision-making process, as well as the basis for the licensee's integrated decision-making process conclusion, should be clearly documented. The reviewer should evaluate this documentation to see if there is adequate technical justification for the licensee's decisions.

Specific acceptance guidelines for use of Expert Panels are contained in Appendix B of reference 3.

B. IMPLEMENTATION, PERFORMANCE MONITORING, AND CORRECTIVE ACTION

1. Program Implementation

For either high or low safety significant components that will be tested in accordance with the current NRC-approved Code test frequency and method requirements, no specific implementation schedule is required. The test frequency should be included in the licensee's RI-IST program.

For either high or low safety significant components that will employ NRC-

DRAFT FOR COMMENT

endorsed ASME Code cases, implementation of the revised test strategies should be documented in the licensee's RI-IST program.

For any alternate test strategies proposed by the licensee, the licensee should submit a relief request to the NRC (reference Section III.A.4).

For low safety significant components that will be tested at a frequency less than the Code test frequency which are exercised as a result of testing, routine maintenance, or normal plant operation and have acceptable performance histories, the licensee should group these components and test them on a staggered basis. Grouping is acceptable provided it complies, for example, with the guidance contained in NRC Generic Letter 89-04, Position 2 for check valves; Supplement 6 to NRC Generic Letter 89-10 and Section 3.5 of ASME Code Case OMN-1 for motor-operated valves; or other documents endorsed by the NRC.

Component monitoring that is performed as part of the Maintenance Rule implementation can be used to satisfy monitoring as described in the RI-IST program guidance. In these cases, the performance criteria chosen have to be compatible with the RI-IST guidance provided in Reference 2.

For low safety significant components that will be tested at a frequency less than the licensee's current Code test frequency which are not exercised as a result of non-Code required system or component testing, routine maintenance, or normal plant operation and have acceptable performance histories, the licensee should increase the test interval in a step-wise manner. If no time-dependent failures occur, then the interval can be gradually extended until the component, or group of components if tested on a staggered basis, is tested at the maximum proposed extended test interval.

2. Performance Monitoring of IST Equipment

The acceptance guidelines for this item consists of evaluating the licensee's proposed performance monitoring process to ensure that it has the following attributes:

- enough tests are included to provide meaningful data;
- the test is devised such that incipient degradation can reasonably expected to be detected; and
- the licensee trends appropriate parameters as required by the ASME Code or ASME Code case and as necessary to provide validation of the PRA.

Assurance must be established that degradation is not significant for components that are placed on an extended test interval, and that failure rate

DRAFT FOR COMMENT

assumptions for these components are not compromised. It must be clearly established that the test procedures and evaluation methods are implemented which provide reasonable assurance that degradation will be detected and corrective action taken.

3. Feedback and Corrective Action Program

The licensee's corrective action program for this application is acceptable if it contains a performance-based feedback mechanism to ensure that if a particular component's test strategy is adjusted in a way that is ineffective in detecting component degradation and failure, the IST program weakness is promptly detected and corrected.

The licensee's corrective action program should evaluate RI-IST components that either fail to meet the test acceptance criteria or are otherwise determined to be in a nonconforming condition (e.g., a failure or degraded condition discovered during normal plant operation).

The licensee's corrective action procedures should:

- (a) comply with 10 CFR 50, Appendix B, Criterion XVI, Corrective Action
- (b) determine the impact of the failure or nonconforming condition on system/train operability since the previous test,
- (c) determine and correct the root cause of the failure or nonconforming condition (e.g., improve testing practices, repair or replace the component),
- (d) assess the applicability of the failure or nonconforming condition to other components in the IST program (including any test sample expansion that may be required for grouped components such as relief valves),
- (e) correct other susceptible similar IST components as necessary,
- (f) assess the validity of the PRA failure rate and unavailability assumptions in light of the failure(s), and
- (g) consider the effectiveness of the component's test strategy in detecting the failure or nonconforming condition. Adjust the test frequency and/or methods, as appropriate, where the component (or group of components) experiences repeated failures or nonconforming conditions.

The corrective action evaluations should be provided to the licensee's PRA group so that any necessary model changes and re-grouping are done as might be appropriate. The effect of the failures on plant risk should be evaluated as well as a confirmation that the corrective actions taken will restore the plant risk to an acceptable level.

The RI-IST program documents should be periodically revised to document any RI-IST program changes resulting from corrective actions taken.

4. Periodic Reassessment

The test strategy for IST components should be periodically, at least once

DRAFT FOR COMMENT

every two refueling outages, assessed to take into consideration results of inservice testing and new industry findings. Plant specific data by itself should not be the sole basis to determine component operability because the sample size will, in most cases, not be sufficient. Therefore, the IST PRA model should also reflect industry experience. (See Section III.A.8.e)

5. Formal Interactions With the NRC

The licensee can make changes to their RI-IST program that are consistent with the process and results that were reviewed and approved by the NRC staff. For example:

- Changes to component groupings, test intervals, and test methods that do not involve a change to the overall RI-IST approach (either traditional engineering or PRA analyses), where the overall RI-IST approach was reviewed and approved by the NRC do not require specific (i.e., additional) review and approval prior to implementation.
- Component test method changes involving the implementation of an NRC-endorsed ASME Code, NRC-endorsed Code case, or published NRC guidance which were approved as part of the RI-IST program, do not require prior NRC approval.
- Test method changes that involve deviation from the NRC-endorsed Code requirements require NRC approval prior to implementation.
- Changes to the risk-informed IST program that involve programmatic changes (e.g., changes to the plant probabilistic model assumptions, changes to the grouping criteria or figures of merit used to group components, changes in the Acceptance Guidelines used by the licensee's integrated decision-making process (e.g., expert panel)) require NRC approval prior to implementation.

Changes to a licensee's RI-IST program should also be evaluated using change mechanisms described in the regulations (e.g., 10 CFR 50.55a, 10 CFR 50.59), as appropriate, to determine if prior NRC staff review and approval is required prior to implementation. In addition, changes to a licensee's approved RI-IST program (e.g., a change to a component's categorization) that could affect the results that were reviewed and approved by the NRC staff (e.g., the change in risk associated with implementation of the RI-IST program), should be evaluated to ensure that the basis for the staff's approval has not been compromised.

The licensee is not required to submit regular IST program updates. The licensee may elect to submit program updates in situations that may help the staff evaluate pending requests for relief or authorization, or when there have been significant program changes that do not require review.

DRAFT FOR COMMENT

IV. REVIEW PROCEDURES

A. REVIEW OF THE LICENSEE'S ENGINEERING EVALUATION

1. Evaluation of Proposed Changes to the Current Licensing Basis

Verify that the licensee reviewed licensing basis documents to identify proposed changes to the IST program that would alter the current licensing basis of the plant. On a component-specific basis, the licensee should have identified each instance where the proposed IST program change would affect the current licensing basis of the plant, identified the source and nature of the commitment (or requirement), and documented the basis for the acceptability of the proposed change. If the current licensing basis was not affected by the proposed IST program changes, the licensee should have so indicated in its risk-informed IST program description.

On a component-specific basis, the reviewer should evaluate the acceptability of each proposed change that impacts the CLB. Acceptability should consider the original acceptance conditions, criteria, and limits as well as the risk significance of the component. Ensure that the licensee explicitly and adequately addressed each of the key safety principles.

Verify that the licensee reviewed commitments related to outage planning and control to verify that they were appropriately reflected in the licensee's component grouping. Spot check to determine if components that play an integral role in the licensee's plans and procedures for maintaining the key shutdown safety functions are in the group of components that are candidates for more focused inservice tests (i.e., high safety significant component category).

2. IST Program Scope

Review the proposed IST program and verify the following:

- For selected systems, verify that components that perform a safety-related function(s) are in the proposed RI-IST program.
- Components categorized as "high safety significant" are included in the RI-IST program, regardless of their status in the licensee's current IST program.

3. IST Program Changes

a. General

Verify that the licensee reevaluated the test frequency (and methods as applicable) for high safety significant components that were the subject of a deferred test justification, approved relief request, or NRC authorized alternative test. Review resubmitted relief requests and requests that

DRAFT FOR COMMENT

alternatives be authorized, along with risk-related insights.

On a sampling basis, verify that the licensee considered component design, service condition, and performance as well as risk insights, in establishing the technical basis for each component's (or group of components) test interval. The licensee's rationale for the proposed change in test interval and its relationship to expected time to failure should be reviewed. Verify that the proposed test intervals are supported by applicable generic or plant-specific failure rate data. Verify that proposed test intervals are significantly less than the expected time to failure of the components in question (e.g., an order of magnitude less). Alternatively, spot check the licensee's calculations to ensure that adequate component capability exists, above that required during design basis conditions, such that component operating characteristics over time do not result in reaching a point of insufficient margin before the next scheduled test activity. Verify that the inservice test intervals are not extended beyond once every 5 years or 3 refueling outages (whichever is longer) without specific compelling documented justification. Extensions beyond 5 years or 3 refueling outages should be considered as component performance data at extended test intervals is acquired and as PRA technology improves.

On a sampling basis, verify that IST components (i.e. with the exception of check valves) are exercised or operated at least once every refueling cycle. Check to see if components in the following categories are exercised more frequently than once per operating cycle, if practical:

- a) Components with high risk significance;
- b) Components in adverse or harsh environmental conditions; or
- c) Components with any abnormal characteristics (operational, design, or maintenance conditions).

If the licensee chooses to use the alternative described in reference 2 for implementing a RI-IST program, verify that the licensee made a commitment to adopt enhanced test strategies as described in risk-based IST Code cases developed by ASME, as endorsed by the NRC. If the licensee chooses not to adopt one or more of these Code cases, review the licensee's written technical justification outlining why it was impractical to implement the risk-informed Code Case strategy as well as the licensee's proposed alternative test strategy.

Verify that the licensee's RI-IST program identifies and tests components in the high safety significant category that are not in the licensee's current IST program commensurate with their safety significance or that the licensee has demonstrated that a suitable search for such components was conducted. These components should be tested in accordance with the ASME Code where practical, including compliance with all administrative requirements. Where ASME Section XI or O&M testing is not practical, alternative test methods to ensure operational readiness and to detect component degradation (i.e., degradation associated with failure modes identified as being important in the

DRAFT FOR COMMENT

licensee's PRA) should be proposed by the licensee. These alternative test strategies should be reviewed and approved by the NRC prior to implementation of the RI-IST program at the plant (see SRP section V. D.).

On a sampling basis, confirm that changed test strategies do not result in violating TS requirements, or that an appropriate amendment request is submitted.

b. Changes to Test Interval (Only)

Verify that the process used by the licensee to group components [i.e., components that are candidates for having their inservice test requirements relaxed and components that should be subjected to more frequent (e.g., quarterly) and effective inservice tests] is consistent with the acceptance guidelines specified in Section III.A.3.b and that appropriate commitments to adopt enhanced test strategies have been made (i.e., if the alternative described in reference 2 for implementing a RI-IST program is proposed by the licensee).

c. Changes to Test Interval and Methods

Verify that tests performed for the components within the scope of the RI-IST program meet the enhanced ASME Code test strategies (i.e., test method and frequency) as endorsed by the NRC, except where NRC has either granted relief or authorized an alternative test strategy.

4. Relief Requests and Technical Specification Amendments

The regulation (or alternative that was authorized by the NRC) that permitted the licensee to implement the overall RI-IST program will, in part, allow licensees to increase the testing interval (and possibly relax test methods) of components categorized, through the use of their PRA and integrated decision-making process, as low safety significant. Approval of the alternative includes evaluation and approval of the process to identify low safety significant components and adjust their test frequencies (or test methods) commensurate with their previous service and maintenance histories and existing environmental conditions. Therefore, individual component relief requests are not required to adjust the test interval of individual components that are categorized as having low safety significance (i.e., because the licensee's implementation plans for extending specific component test intervals should have been reviewed and approved by the NRC staff as part of their RI-IST program submittal). Similarly, if the proposed alternative includes improved test strategies to enhance the test effectiveness of low and high safety significant components, such as the use of ASME Code Case OMN-1, "Alternate Rules for Preservice and Inservice Testing of Certain Electric Motor Operated Valve Assemblies in LWR Power Plants, OM-Code - 1995 Edition; Subsection ISTC" then additional relief from the Code requirements (i.e., beyond staff approval of the licensee's RI-IST program describing the licensee's intention to adopt such a Code case) is not required (See footnote

DRAFT FOR COMMENT

6 to 10 CFR 50.55a).

For high and low safety significant components not tested in accordance with the Code test method requirements or NRC endorsed Code Case, specific relief would be required from the applicable Code requirements. Relief would also be required from the Code test frequency requirements for high safety significant components not tested at the Code-required frequency. (High safety significant components are expected to be maintained at Code-required frequencies unless specific relief exists or adjustment is bounded by Generic Letter 89-04.)

- a. Verify that requests for relief or approval for alternative testing have been submitted to the NRC. Verify that the licensee has submitted technical specification amendment requests for proposed changes that impact technical specification.
- b. Review the basis for requests for relief and alternatives and assess the adequacy of the implementation of the alternative testing.
- c. Review the justification for deferring testing of high safety significant components to cold shutdowns or refueling outages.

5. Quality of the PRA for IST Application

The reviewer should establish that for IST applications, special attention has been paid to quantification of the failure probability of IST components in light of IST program attributes (e.g., test interval), and that special attention has been paid to quantification of the failure probability of compensating SSCs.

Fault Exposure Time for IST Components:

Reviewers must ensure that the fault exposure time credited in the PRA is reasonable in light of the IST interval and other activities. In general, the mean fault exposure time will be taken to be 1/2 of the test interval. Some analyses may apply a fault exposure time other than this: a different fault exposure time for a given component might be claimed as a result of credit taken for non-IST validation of the performance of the component, perhaps by virtue of system challenges, or an IST test on a different component that implicitly requires functioning of the subject component and would therefore reveal a failed state of the subject component. The reviewer should establish that the licensee has identified a basis for every fault exposure time modeled, and that commitments are in place wherever a fault exposure time is determined by a programmatic activity. Where a fault exposure time is the result of tests on other components, the reviewer should verify that there is assurance that these other tests will be performed and that the behavior of the subject component will be surveilled in the course of these tests. Where a fault exposure time is the result of system challenges, the reviewer should verify that this challenge frequency is consistent with system challenge

DRAFT FOR COMMENT

frequencies modeled elsewhere in the PRA.

Failure Rates for IST Components:

The reviewer should establish that in general, failure rates for components are consistent with plant-specific data, except that failure rates that are appreciably less than generic data (e.g., those on the order of a factor of 3 or more lower than generic data) should be justified. To use the lower plant-specific failure rate, it must be demonstrated that the plant-specific failure rate data came from a population statistically different from the generic population and a mechanistic explanation should be provided.

The reviewer should ascertain whether the failure rate takes account of special environmental stresses or aging. If not, this should figure in the evaluation of the performance monitoring and feedback activity (see Sections III.B.3 and IV.B.3).

Basic Event Probabilities of Compensating SSCs:

Events that appear jointly in minimal cut sets with IST components (compensating SSCs) must be quantified appropriately or else perspective on the significance of IST components will be distorted. Depending on the form of PRA documentation, this can be relatively difficult for reviewers to spot check; reviewers should therefore verify that as part of IST applications, licensees warrant that the apparent significance of IST events is not distorted by inappropriate quantification of compensating events. Note that PRA updates may have been performed to boost the credited performance of compensating SSCs in anticipation of the need to justify relaxed IST intervals. This is acceptable, and need not prompt special staff attention beyond that allocated generally to review of baseline risk profiles, provided that the licensee makes programmatic commitments appropriate to the level of performance claimed.

Common Cause Failures:

Reviewers should check that licensees have appropriately modeled CCF of groups of similar components that are proposed for relaxation and that are mutually redundant. This is discussed more in detail in Section 4.2.4.2 of reference 2.

6. Modeling of the Effects of IST on PRA Basic Events

The review procedure for the modeling of the effects of IST on the risk model involves the following steps:

- Characteristics of the model used to evaluate the risk significance extending selected component test intervals is compared against those considered acceptable as defined in Section III.B.2,

DRAFT FOR COMMENT

- The reviewer establishes that the licensee looked for ways to improve test effectiveness,
- Data and analysis used to support the model are reviewed and compared with independent data sources and analysis.

7. Categorization of Components

Results from risk categorization can be used directly for identifying the high risk significant components (e.g., for the identification of risk outliers, or for the identification of SSCs where more resources can be allocated). However, when risk importance measures are used to group components as low risk significant, additional evaluations, sensitivity studies and other considerations as discussed in Section III.A.7 have to be taken into account. Review procedures for component risk categorization are provided in Appendix C of the general SRP for risk informed regulation.

8. Other Technical Issues

a. Initiating Events

For most aspects of the general case of IST changes on initiating event frequency, the reviewer is not expected to accept or reject the analysis through a process of independent validation of the licensee's evaluation of the effect of IST program changes on initiating event frequency. Rather, the reviewer is expected to look for evidence that the licensee

- considered the effect of IST changes on initiating events that were analyzed (not screened out),
- considered whether the IST changes would affect the frequencies of initiating events previously screened out from the analysis.

Note that the latter step logically requires that there have been documentation of the basis for screening out of initiating events.

However, if a licensee argues for a reduction in testing or a change in protocol based on adverse risk effects of testing, the reviewer should spot check the calculations, especially if other plants of the same type have not drawn similar conclusions.

b. Dependencies and Common Cause Failures

The reviewer should check to confirm that potential CCFs which involve IST components 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. As a minimum, the CCF groups should include: redundant standby pumps; redundant MOVs/AOVs that change state; redundant check valves; and any other components that

DRAFT FOR COMMENT

change state in order to support IST component operability.

The reviewer should verify that plant specific experience which involve the failure of two or more components from the same cause was analyzed and incorporated into the model where appropriate.

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

Reviewers should check that licensees have established that performance monitoring is capable of detecting CCF before multiple failures are allowed to occur subsequent to an actual system challenge.

c. Uncertainty and Sensitivity Analyses

The following are review considerations for the licensee evaluation of uncertainties:

- If the estimated risk change due to implementation of the IST program is a bounding estimate, then the reviewer should confirm that the models and data assumptions used do indeed produce a demonstrably conservative estimate.
- If the licensee contends that the estimated risk change due to implementation of the IST program is a best estimate, then the reviewer needs to establish that uncertainty is addressed for the change. This argument must 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.

d. Human Reliability Analysis

The comprehensive review of human reliability modeling is treated in the general Reg Guide and general SRP. For IST applications, the review can be more focused. The IST-specific aspects include errors specifically related to testing, and quantification of compensating human actions.

Errors Specifically Related To Testing:

Two types of errors are of interest here. The first is errors during testing that leave equipment unavailable until the condition is discovered during a subsequent test or until the equipment is demanded (i.e., a restoration error). In some PRAs, such errors are included in the data base that is used for the equipment failure rate. The licensee should have verified that this is the case. If such errors are not included, they should have been considered separately. If they were considered separately, then the

DRAFT FOR COMMENT

assumptions, models, and data used should be consistent with those that are generally accepted.

The second type of error is associated with error during recovery (e.g., failure to actuate an alternative system train). As indicated previously, the only recovery allowed for present purposes is manual actuation of alternate available equipment to work around failed equipment when a demand occurs and the normal equipment response fails. For this recovery situation, human errors must be considered, and they should reflect the time available to actuate the alternate available equipment, the procedures and training available, and adverse environmental factors (access to equipment, local temperatures and radiation levels, etc.).

Quantification of Compensating Human Actions:

This refers to the credit taken for human actions for purposes of deciding on IST changes. The reviewer should confirm that credit for compensating human actions is limited to proceduralized actions taken to actuate systems; repair of failed equipment is not to be considered. The intent of this review step is to ensure that licensees do not reduce IST on the basis of arguably speculative and relatively uncertain quantification of recovery probabilities. That is, acceptability of IST program changes should be assessed without credit for such recovery probabilities. Quantification of the baseline for purposes of deciding the acceptability of the overall risk profile and deciding on the allowed risk increment may be performed on the basis of credit for such actions.

e. Use of Plant-Specific Data

Appendix A of the reference 3 (SRP Chapter 19) provides procedures for the review of generic and plant-specific data used in support of the licensee's PRA.

9. Evaluating the Overall Effect of Proposed Changes on Plant Risk

Reference 3 (SRP Chapter 19) provides review procedures for the acceptance of RI-IST program changes.

10. Integrated Decision Making

There are no explicit criteria for dispositioning the results of traditional engineering and probabilistic analyses which may conflict with one another. The reviewer should evaluate the licensee's integrated decision-making process records associated with these conflicts. The licensee's integrated decision-making process records should clearly identify all factors considered by that process and the basis for conclusion. On a sampling basis, the reviewer should conduct an independent evaluation to determine if the licensee's conclusion has sufficient technical basis. The reviewer's determination that

DRAFT FOR COMMENT

the proposed alternative will provide "an acceptable level of quality and safety" [ref. 10 CFR 50.55a (a)(3)(i)] should be based on the independent assessment. The reviewer should consider the following factors in trying to reach a conclusion relative to the acceptability of the licensee's proposed RI-IST program:

- a. Does the proposed RI-IST program meet the current regulations? [This principle applies unless the proposed change is explicitly related to a requested exemption or rule change.]
- b. Is defense in depth philosophy maintained?
- c. Are sufficient safety margins maintained?
- d. Are proposed changes in risk, and their cumulative effect, small and within the NRC Safety Goals?
- e. Has the licensee proposed performance-based implementation and monitoring strategies that address uncertainties in analysis models and data and provide for timely feedback and corrective action?

More detailed guidance for reviewing the integrated decision making process is provided in Appendix B of Reference 3.

B. REVIEW OF IMPLEMENTATION, PERFORMANCE MONITORING, AND CORRECTIVE ACTION

1. Program Implementation

On a sampling basis, the reviewer should verify that the following information is provided for each component in the RI-IST program:

High Safety Significant Components:

- a) component test method and interval
- b) ASME Code Case, if applicable
- c) technical specification amendment, if applicable
- d) relief request, if applicable

Low Safety Significant Components:

- a) component test method and interval with justification for extending interval if greater than interval specified in ASME Code
- b) ASME Code Case, if applicable
- c) technical specification amendment, if applicable
- d) relief request, if applicable
- e) grouping definition and justification
- f) staggered test justification for specific low safety significant components
- g) justification for test extensions for the remaining low safety

DRAFT FOR COMMENT

significant components

High and low safety significant components that will continue to be tested in accordance with the ASME Code requirements for the licensee's Code of record, or ASME Code Cases that have been endorsed by the NRC, require no further evaluation.

The justification for extending the low safety significant component frequencies should be reviewed for adequacy to verify that the extension is appropriate. Staggered implementation schedules should be evaluated to ensure that component tests are distributed as equally as possible over the entire test interval.

The test intervals of the low safety significant components should be included in the RI-IST program for review. Low safety significant components that are grouped should have their respective groups identified in the RI-IST program. The implementation schedule should be described in the RI-IST program. Implementation of interval extension for low safety significant components may begin at the discretion of the licensee subsequent to NRC approval of risk informed IST program. Component corrective action procedures (see SRP section IV.B.3) should be in place for low safety significant components being tested on a staggered basis prior to implementation of any interval extensions.

For low safety significant components tested on a staggered basis, the licensee should have documented the approach to exercising to which each component in the group is subjected (where appropriate) as a result of plant operation or testing of other components to assess the justification for allowing the component to be tested on a staggered basis. The overall test interval for the low safety significant components in the group should also be justified. The adequacy of the component groupings should be verified. The establishment of the staggered test interval should be based on the maximum allowable interval for all the components in a particular group. Each component in the group should have the same designated test interval.

For low safety significant components exercised only during inservice testing, the current testing interval should be defined in the RI-IST program. In addition, a schedule should be available that shows the planned test interval of each individual low safety significant component being gradually extended to the test interval selected by the licensee and described in the approved program. An acceptable method for extending the test interval for this subset of low safety significant components is by gradually extending the test interval by a set amount (i.e., equal or successively smaller steps) until the maximum approved test interval is reached. The licensee could propose an alternative phased approach to extend the test interval. When the maximum allowed test interval is achieved in the absence of time-dependant test failures, then the components may be grouped and tested on a staggered basis. Section III.B.3 discusses adjusting (i.e., shortening) the test interval when a component experiences repeated test failures.

DRAFT FOR COMMENT

Verify that the licensee has plant corrective action and feedback procedures developed (see Section IV.B.3) to ensure that testing failures are fed back to the plant licensee's integrated decision-making process and IST coordinator for reevaluation and possible adjustment to the component's grouping and test strategy.

Verify that the licensee has a program and schedule for converting from the old IST program to the RI-IST program.

2. Performance Monitoring of IST Equipment

The review procedures consist of the following steps:

The performance monitoring program is identified in the licensee's proposal for RI-IST.

The program is reviewed to determine whether it includes a test program which will provide sufficient data to detect component degradation in a timely manner as described in Section III.B.2.

3. Feedback and Corrective Action Program

The reviewer should review the licensee's corrective action procedures to verify that it is initiated by component failures that are detected by the IST program as well as by other mechanisms (e.g., normal plant operation, inspections).

Verify that the licensee's corrective action procedures meets the acceptance guidelines specified in Section III.B.3.

Verify that corrective action evaluations are provided to the licensee's PRA group so that any necessary model changes and re-grouping can be done by the PRA group if appropriate.

Verify that procedures are in place to ensure that corrective actions affecting the IST program get documented, as appropriate, in the licensee's RI-IST program.

4. Periodic Reassessment

Review the licensee's procedures for conducting the periodic risk-informed IST program review to ensure that it:

prompts the licensee to conduct overall program assessments periodically (i.e., at least once every two refueling outages) to reflect changes in plant configuration, component performance, test results, industry experience, and to reevaluate the effectiveness of the IST program,

prompts the licensee to compare actual component conditions/performance

DRAFT FOR COMMENT

to predicted levels to determine if component performance and conditions are acceptable (i.e., as compared to predicted levels). If performance or conditions are not acceptable then the cause(s) should be determined and corrective action implemented,

prompts the licensee to review and revise as necessary the assumptions, reliability data, and failure rates used to group components to determine if component groupings have changed, and

prompts the licensee to reevaluate equipment performance (based on both plant-specific and generic information) and test effectiveness to determine if the inservice test program should be adjusted (Plant-specific data should be incorporated into the generic data using appropriate updating techniques).

Verify that the licensee has incorporated the results of its corrective action program for IST program components into its periodic IST program reassessment.

Verify that the licensee has procedures in place to identify the need for more emergent RI-IST program updates (e.g., following a major plant modification, or significant equipment performance problem).

The periodic RI-IST program review may be addressed in conjunction with the plant's periodic PRA updates, industry operating experience programs, the Maintenance Rule program, and other risk-informed program initiatives.

5. Formal Interactions With the NRC

Verify that the licensee has a process or procedures in place to assure that changes that meet the acceptance guidelines in Section III.B.5 above get reviewed and approved by the NRC staff prior to implementation.

V. EVALUATION FINDINGS

Before the reviewer writes findings in each of the review areas as discussed below, the reviewer should write an introduction to the safety evaluation that describes the proposed change in terms of:

- the particular components that would be affected by the proposed changes in IST strategy,
- the plant systems involved with the proposed changes in IST strategy,
- the physical change in testing strategy proposed for each component or group of components,
- its affect on the current licensing basis, and

DRAFT FOR COMMENT

- its overall affect on plant risk.

A. ENGINEERING EVALUATION

1. Evaluation of Proposed Changes to the Current Licensing Basis

The reviewer verifies that sufficient information is provided in accordance with the requirements of this SRP section and that the evaluation supports conclusions of the following type, to be included in the staff's safety evaluation report:

On a component-specific basis, the staff has reviewed each IST program change as it affects the current licensing basis of the plant. In conducting its review, the staff considered the original acceptance conditions, criteria, and limits as well as the risk significance of the component. Due consideration was given to diversity, redundancy, defense in depth, safety margins, and other aspects of the General Design Criteria. Having conducted this review, the staff finds that the IST program changes proposed by the licensee are acceptable.

The licensee has reviewed commitments related to outage planning and control to ensure that components that play an integral role in the licensee's plans and procedures for maintaining the key shutdown safety functions are in the group of components that should be subjected to more frequent and effective inservice tests. The staff finds this to be acceptable.

IST-related commitments appear to be adequately modeled in the licensee's PRA analysis, or otherwise addressed.

2. IST Program Scope

The reviewer verifies that sufficient information is provided in accordance with the requirements of this SRP section and that the evaluation supports conclusions of the following type, to be included in the staff's safety evaluation report:

The staff concludes that the scope of the applicant's risk-informed inservice test program is acceptable and is consistent with the guidance provided in Regulatory Guide 1062. This conclusion is based on the applicant having provided a test program to ensure that safety-related components, as well as other components that are important to plant risk, can reasonably be expected to be capable of performing their intended function throughout the life of the plant.

3. IST Program Changes

a. General

DRAFT FOR COMMENT

The reviewer verifies that sufficient information is provided in accordance with the requirements of this SRP section and that the evaluation supports conclusions of the following type, to be included in the staff's safety evaluation report:

The licensee reevaluated the testing frequency (and methods as applicable) for high safety significant components that were the subject of an approved relief request, or NRC authorized alternative test. The licensee submitted revised relief requests and requests that alternatives be authorized for these components, along with risk insights associated with the proposed test strategy. The licensee identified technical specification changes needed to implement the RI-IST program and has submitted technical specification amendment requests as appropriate. These requests were reviewed by the NRC staff and found to be acceptable [each instance should be explicitly addressed in the SE].

The licensee considered component design, service condition, and performance, as well as risk insights in establishing the test interval for low safety significant components. The proposed test intervals for low safety significant components were significantly less than the expected time to failure of the components in question (e.g., an order of magnitude less). Alternatively, the licensee ensured that adequate component capability existed, above that required during design basis conditions, such that component operating characteristics over time will not result in reaching a point of insufficient margin before the next scheduled test activity. The inservice test intervals for components were generally not extended beyond once every 5 years or 3 refueling outages (whichever is longer). In every instance where the interval was extended beyond 5 years or 3 refueling outages (whichever is longer), the licensee provided a specific compelling documented justification that was found to be acceptable to the staff [each instance should be explicitly addressed in the SE].

The licensee's proposed RI-IST program ensures that each IST component (i.e. with the exception of check valves) is exercised or operated at least once every refueling cycle. Components in the following categories are generally exercised more frequently than once per operating cycle:

- a) Components with high risk significance;
- b) Components in adverse or harsh environmental conditions; or
- c) Components with any abnormal characteristics (operational, design, or maintenance conditions).

The licensee also made a commitment to either adopt enhanced test strategies as described in risk-based IST Code cases developed by ASME, as endorsed by the NRC, or request authorization from the NRC to perform an alternative test strategy.

DRAFT FOR COMMENT

Finally, where the licensee has identified high safety significant components that are not in the licensee's current IST program, the licensee has either committed to test these components in accordance with the current ASME Code or has proposed an alternative test strategy that has been reviewed and approved by the NRC staff.

b. Changes to Test Interval ((y)

The licensee's proposed RI-IST program is found to be acceptable because it:

- a) appropriately identifies components whose test interval should be decreased as well as components whose test interval might be extended,
- b) considers IST test effectiveness in determining whether components are candidates for having their inservice test requirements relaxed.

The reviewer should specify which components will be tested at a shorter interval.

c. Changes to Test Interval and Methods

The licensee's proposed RI-IST program is found to be acceptable because it appropriately identifies components whose test strategy should be more focused as well as components whose test strategy might be relaxed. The reviewer should identify (or characterize) which components will be subjected to more focused testing and describe the revised test strategy for these components.

4. Relief Requests and Technical Specification Amendments

The reviewer verifies that sufficient information is provided in accordance with the requirements of this SRP section and that the evaluation supports conclusions of the following type, to be included in the staff's safety evaluation report:

The licensee's RI-IST program is testing high safety significant components in accordance with the Code test frequency and method requirements or has a relief request approved or submitted for approval. In addition, the licensee is testing low safety significant components in accordance with the Code test method requirements (although at a extended interval) or has a relief request approved or submitted for approval. The licensee has approved technical specification amendments for all proposed changes that impact technical specification.

5. Quality of the PRA for IST Application

DRAFT FOR COMMENT

The reviewer verifies that sufficient information is provided in accordance with the requirements of this SRP section and that the evaluation supports conclusions of the following type, to be included in the staff's safety evaluation report:

- Fault exposure time is modeled appropriately for IST components. Fault exposure times are appropriately linked to programmatic activities that have been explicitly identified and documented.
- Appropriate failure rates have been used for IST components. Wherever unusually good performance is being claimed, provisional justification has been provided and monitoring will provide ongoing justification.
- The licensee has reviewed the modeling of compensating SSCs, and concluded that it is appropriate and that the significance of IST events is not distorted by modeling of compensating SSCs.
- Common cause failure has been suitably addressed. The licensee has systematically identified all component groups sharing attributes that correlate with CCF potential and that affect IST, either in that they comprise IST components or compensating SSCs. The licensee's performance monitoring program addresses staggered testing of IST components in CCF groups.
- The effects of aging, environmental stresses, and frequency of testing has been addressed, either explicitly in the PRA models or as part of the licensee's integrated decision-making process (e.g., expert panel).

6. Modeling of the Effects of IST on PRA Basic Events

The reviewer verifies that the information provided supports the following conclusions:

- a model for unavailability in terms of fault exposure time exists and was used in the PRA for evaluating the risk significance of extending the selected component test intervals,
- the assumptions provided relative to time dependent degradation of the failure rates for the selected components are justified, and
- the licensee considered enhanced testing as a compensating measure.

7. Categorization of Components

The reviewer verifies that sufficient information is provided in accordance with the requirements of this SRP section and that the evaluation supports conclusions of the following type, to be included in the staff's safety evaluation report:

DRAFT FOR COMMENT

The licensee's integrated decision-making process (e.g., expert panel) on the determination of risk importance of components in the RI-IST program is robust in terms of the "uncertainty" issues like common cause failure modeling and modeling of human reliability.

8. Other Technical Issues

a. Initiating Events

There is positive evidence that the licensee adequately considered the effects of proposed IST changes on the frequencies of initiating events analyzed and the frequencies of initiating events previously screened out. In addition, if the licensee analyzed adverse risk effects of IST activities, and applied these results to justify IST reductions, this analysis was found acceptable. Either the analysis is consistent with previously accepted analyses applicable to this plant type, or the causal modelling of the IST activities' effects on initiating effects was reviewed and found to address appropriately the technical issues described in this SRP under "causal modelling."

b. Dependencies and Common Cause Failures

Evaluation findings should include statements that 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 IST, either in that they comprise IST components or compensating SSCs. The licensee's performance monitoring program addresses staggered testing of IST components in CCF groups.

c. Uncertainty and Sensitivity Analyses

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

An appropriate consideration of uncertainties is provided in support of the proposed risk informed IST program. The licensee showed either that a demonstrably conservative estimate of the change in risk was acceptable, or that the uncertainty in the risk change was small compared to the margin between the estimated change and the allowable change. In the latter case, this was done either by explicit propagation, or by a qualitative analysis showing that no event contributing to the change in risk is subject to significant uncertainty.

d. Human Reliability Analysis

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

- The modeling of human performance is appropriate.

DRAFT FOR COMMENT

- 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).

e. Use of Plant-Specific Data

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

- The failure rates used in the proposed risk informed IST program are appropriate and consistent with Appendix A of SRP Chapter 19, or the deviations are justified.

9. Evaluating the Overall Effect of Proposed Changes on Plant Risk

The reviewer verifies that sufficient information is provided to make the following findings:

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 acceptance guidelines specified in Regulatory Guide DG-1061.

Traditional Engineering Factors

- Traditional engineering analyses and operational considerations do not conflict with the conclusions of the risk analysis.

Cumulative and Synergistic Effects from all Applications

- The cumulative changes in risk are consistent with the guidelines established in DG-1061
- Synergistic effects have been satisfactorily addressed at the component level either
 - 1) by assuring that multiple synergistic relaxations are not applied to a single component, or
 - 2) by noting exceptions to this, and convincingly justifying them case

DRAFT FOR COMMENT

by case.

Implementation of a Monitoring Process

- The monitoring process will produce sufficient data that can support the PRA input and assumptions that were used as the basis for the IST risk acceptance.

10. Integrated Decision Making

If the licensee's proposed alternative is acceptable in light of the current licensing basis of the plant and the safety significance of the component,

AND

if the licensee's risk-informed IST program meets the detailed acceptance guidelines specified in this SRP,

then the staff should be able to reach the following general conclusion:

The licensee's proposed risk-informed IST program is authorized as an alternative to the ASME Code required IST program (e.g, including test frequency, test methods, and program scope requirements) pursuant to § 50.55a(a)(3)(i) based on the alternative providing an acceptable level of quality and safety.

B. RISK-INFORMED IST PROGRAM IMPLEMENTATION, PERFORMANCE MONITORING, AND CORRECTIVE ACTION

1. Program Implementation

The reviewer verifies that sufficient information is provided in accordance with the requirements of this SRP section and that the evaluation supports conclusions of the following type, to be included in the staff's safety evaluation report:

For components in the high safety significant category, the licensee is either going to continue to test these components in accordance with the current ASME Code of record for the facility (i.e., test frequency and method requirements) or has proposed an alternative test strategy that is acceptable to the staff (via either an NRC-endorsed ASME Code case or plant specific relief request). Testing strategies are adequately described in the licensee's RI-IST Program Plan and were found to be acceptable.

For components in the low safety significant category, the licensee is either going to continue to test these components in accordance with the current ASME Code of record for the facility or has proposed an alternative test strategy that was found acceptable to the staff.

DRAFT FOR COMMENT

Low safety significant components that will be tested at a frequency less than the Code test frequency, which are also exercised as a result of plant operation or other system/component testing, may be grouped and tested at an extended test interval only if the interval can be justified based on past component performance. These components will be tested on a staggered basis at roughly equal time intervals. Corrective action procedures will ensure that failures or nonconforming conditions that may apply to other components in the group get evaluated and corrected. Component grouping was found to be consistent with guidance provided in NRC Generic Letter 89-04 or other documents endorsed by NRC.

Low safety significant components that will be tested at a frequency less than the current Code test frequency, which are not exercised as a result of non-Code required system or component testing, routine maintenance, or normal plant operation, will also only have their test interval extended if it can be justified based on past component performance. The licensee will gradually extend the test interval by doubling the test interval for successive tests until the component is tested at the proposed extended test interval. If no age-dependent failures occur, then the components will be grouped and tested on a staggered basis. Corrective action procedures will ensure that test interval and/or methods, as appropriate, get adjusted where the component (or group of components) experiences repeated failures or nonconforming conditions.

The licensee has plant corrective action and feedback procedures developed to ensure that testing failures are fed back to the plant licensee's integrated decision-making process (e.g., expert panel) and IST coordinator for reevaluation and possible adjustment to the component's grouping and test strategy.

The licensee has appropriate plans and schedules for converting from the old IST program to the new RI-IST program at their facility.

2. Performance Monitoring of IST Equipment

The reviewer verifies that the information provided supports the following conclusions:

a performance monitoring program exists which covers all components which are placed on an extended IST schedule,

the program responds to the attributes specified in Section III.B.2, and

the licensee is committed to maintain the program as part of its RI-IST initiative.

3. Feedback and Corrective Action Program

DRAFT FOR COMMENT

The reviewer verifies that sufficient information is provided in accordance with the requirements of this SRP section and that the evaluation supports conclusions of the following type, to be included in the staff's safety evaluation report:

The staff concludes that the licensee's corrective action program is acceptable for implementation with the RI-IST program because it contains a performance-based feedback mechanism to ensure that if a particular component's test strategy is adjusted in a way that is ineffective in detecting component degradation and failure, the IST program weakness will be promptly detected and corrected.

4. Periodic Reassessment

The reviewer verifies that sufficient information is provided in accordance with the requirements of this SRP section and that the evaluation supports conclusions of the following type, to be included in the staff's safety evaluation report:

The staff concludes that the licensee's procedures for periodic reassessment of its risk-informed IST program are acceptable because the licensee's procedures for periodic reassessment ensure that the licensee's test strategies are periodically [specify periodicity not to exceed once every two refueling outages] assessed to incorporate results of inservice testing and new industry findings.

5. Formal Interactions With the NRC

The reviewer verifies that sufficient information is provided in accordance with the requirements of this SRP section and that the evaluation supports conclusions of the following type, to be included in the staff's safety evaluation report:

The staff concludes that the licensee has an adequate process or procedures in place to ensure that RI-IST program changes of the following types get reviewed and approved by the NRC prior to implementation.

- Test method changes that involve deviation from the NRC-endorsed Code requirements.
- Changes to the risk-informed IST program that involve programmatic changes (e.g., changes to the plant probabilistic model assumptions, changes to the grouping criteria or figures of merit used to group components, changes in the Acceptance Guidelines used by the licensee's integrated decision-making process (e.g., expert panel)).

Changes to component groupings, test intervals, and test methods that do

DRAFT FOR COMMENT

not involve a change to the overall RI-IST approach (either traditional engineering or PRA analyses), where the overall RI-IST approach was reviewed and approved by the NRC do not require specific (i.e., additional) review and approval prior to implementation.

Component test method changes involving the implementation of an NRC-endorsed ASME Code, NRC-endorsed Code case, or published NRC guidance which were approved as part of the RI-IST program, do not require prior NRC approval.

VI. RISK-INFORMED IST PROGRAM DOCUMENTATION

The reviewer should review the licensee's submittal to assure that it contained the documentation necessary to conduct the review described in this SRP (i.e., the documentation described in Section 6 of DG-1062). The RI-IST program and its updates should be maintained on site and available for NRC inspection consistent with the requirements of 10 CFR 50, Appendix B.

The reviewer should also ensure that the cover letter that transmits to the licensee the staff's safety evaluation approving the proposed RI-IST program (i.e., alternative IST program to that prescribed by the ASME Code) contains a statement to the effect that "Failure to comply with the RI-IST program as reviewed and approved by the NRC staff and authorized pursuant to 10 CFR 50.55a(a)(3) [e.g., including scope, test strategy, documentation, and other programmatic requirements] constitutes noncompliance with 10 CFR 50.55a and is enforceable".

VII. IMPLEMENTATION

The preceding 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 proposes an acceptable alternative method for complying with specified portions of this regulatory guide, the method described herein will be used by the staff in its evaluation of risk-informed performance-based changes to the licensee's current licensing basis.

VIII. REFERENCES

1. Draft Regulatory Guide 1061, "An Approach for Plant Specific Risk-Informed Decision Making: General Guidance," January 16, 1997.
2. Draft Regulatory Guide 1062, "Use of PRA in Risk-Informed Inservice Testing," February 4, 1997.
3. Draft Standard Review Plan Chapter 19, "Use of PRA in Regulatory Activities," dated January 16, 1997.

DRAFT FOR COMMENT

4. Nuclear Energy Institute Draft (Revision B) "Industry Guidelines for Risk-Based Inservice Testing" dated March 19, 1996.
5. ASME Research Report (CRDT-Vol. 40-2, Volume 2), "Risk-Based Inservice Testing - Development of Guidelines" dated 1996.
6. NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management," December 1991.
7. ASME Code Case OMN-1, "Alternate Rules for Preservice and Inservice Testing of Certain Electric Motor Operated Valve Assemblies in LWR Power Plants, OM-Code - 1995 Edition; Subsection ISTC."
8. Generic Letter 89-04, "Guidance on Developing Acceptable Inservice Testing Programs," dated April 3, 1989.
9. Generic Letter 89-10, Supplement 6, "Information on Schedule and Grouping, and Staff Responses to Additional Public Questions" dated March 8, 1994.
10. Draft NUREG-1602, "Use of PRA in Risk-Informed Applications"



**UNITED STATES NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR REACTOR REGULATION**

DRAFT FOR COMMENT

Risk-Informed Decisionmaking: Technical Specifications

Draft SRP Chapter 16.1

Revision 13

March 13, 1997

Contacts: N. V. Gilles (301) 415-1180
H. W. Woods (301) 415-6622
M. L. Wohl (301) 415-1181

STANDARD REVIEW PLAN

RISK-INFORMED DECISION MAKING: TECHNICAL SPECIFICATIONS

TABLE OF CONTENTS

| | |
|--|----|
| INTRODUCTION | 1 |
| REVIEW RESPONSIBILITIES | 3 |
| I. AREAS OF REVIEW | 4 |
| II. ACCEPTANCE GUIDELINES | 6 |
| A. Traditional Guidelines | 6 |
| B. Probabilistic Guidelines | 8 |
| III. REVIEW PROCESS | 10 |
| A. Definition of Proposed Change | 10 |
| B. Engineering Evaluations | 11 |
| C. Implementation and Monitoring Program | 17 |
| D. Documentation | 18 |
| IV. EVALUATION FINDINGS | 20 |
| V. IMPLEMENTATION | 21 |
| VI. REFERENCES | 22 |

STANDARD REVIEW PLAN

16.1 RISK-INFORMED DECISION MAKING: TECHNICAL SPECIFICATIONS

INTRODUCTION

Section 182a of the Atomic Energy Act requires that applicants for nuclear power plant operating licenses shall state:

[S]uch technical specifications, including information of the amount, kind, and source of special nuclear material required, the place of the use, the specific characteristics of the facility, and such other information as the Commission may, by rule or regulation, deem necessary in order to enable it to find that the utilization . . . of special nuclear material will be in accord with the common defense and security and will provide adequate protection to the health and safety of the public. Such technical specifications shall be a part of any license issued.

In 10 CFR 50.36, the Commission established its regulatory requirements related to the content of technical specifications (TS). In doing this, the Commission placed emphasis on those matters related to the prevention of accidents and the mitigation of accident consequences; the Commission noted that applicants were expected to incorporate into their TS "those items that are directly related to maintaining the integrity of the physical barriers designed to contain radioactivity" (33 FR 18610). Pursuant to 10 CFR 50.36, TS are required to contain items in the following five specific categories: (1) safety limits, limiting safety system settings and limiting control settings; (2) limiting conditions for operation; (3) surveillance requirements; (4) design features; and (5) administrative controls.

Since the mid-1980s, the NRC has been reviewing and granting improvements to TS based, at least in part, on probabilistic risk assessment (PRA) insights. Some of these improvements have been proposed by the Nuclear Steam Supply System (NSSS) owners groups to apply to an entire class of plants. Many others have been proposed by individual licensees. Typically, the proposed improvements involved a relaxation of one or more allowed outage times (AOTs) or surveillance test intervals (STIs) in the TS.

In its July 22, 1993, final policy statement on TS improvements, the Commission stated that it:

" . . . expects that licensees, in preparing their Technical Specification related submittals, will utilize any plant-specific PSA or risk survey and any available literature on risk insights and PSAs . . . Similarly, the NRC staff will also employ

risk insights and PSAs in evaluating Technical Specifications related submittals. Further, as a part of the Commission's ongoing program of improving Technical Specifications, it will continue to consider methods to make better use of risk and reliability information for defining future generic Technical Specification requirements."

The Commission reiterated this point when it issued the revision to 10 CFR 50.36 in July 1995.

Risk-informed TS submittals primarily deal with permanent changes to TS requirements, i.e., as the name suggests, the requirement is permanently changed when approved, and is applicable for all future occurrences. A one-time change to a TS requirement, where a different requirement is requested for a particular incident, also can use risk-informed evaluations, but it involves slightly different considerations. This Standard Review Plan section focuses on permanent risk-informed changes to TS involving changes in AOTs or STIs. In addition, general guidance for reviewing risk-informed regulatory applications can be found in SRP Chapter 19.0, "Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decision Making. General Guidance."

REVIEW RESPONSIBILITIES

Primary responsibility for evaluating the technical bases for TS modifications resides with the lead technical branch, as specified in SRP Chapter 16.0, "Technical Specifications." Other branches with review responsibility for risk-informed TS change requests include the Probabilistic Safety Assessment Branch, the Technical Specifications Branch, and the appropriate Project Directorate.

L AREAS OF REVIEW

NRC Regulatory Guide DG-1061, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decision on Plant-Specific Changes to the Current Licensing Basis," (Reference 15) describes a four-element approach for evaluating risk-informed regulatory changes. The individual elements are described in detail in Chapter 2 of Regulatory Guide DG-1061. The areas of review for each of these elements for risk-informed TS are discussed below.

Element 1: Define the Proposed Change

The licensee needs to explicitly identify the particular technical specifications that are affected by the proposed change, and identify available engineering studies, methods, codes, and PRA studies that are related to the proposed change. The licensee should consider how such changes will affect conformance with the plant's current licensing basis (CLB)¹. The licensee should also determine how the affected systems, components, or parameters are modeled in the PRA and should identify all elements of the PRA that the change impacts. The licensee should utilize PRA insights to both determine the impact of the change on plant safety and to understand the impact on the licensing basis. Section III.A provides a description of the review process for Element 1.

Element 2: Conduct Engineering Evaluations

The licensee should examine the proposed change to verify that it does not compromise the intent of existing applicable rules and regulations. In addition, the licensee should determine how the change impacts defense in depth aspects of the plant's design and operation, and should determine the adequacy of safety margins following the proposed change. Finally, the licensee should consider how plant and industry operating experience relates to the proposed change, and what potential compensatory measures could be taken to offset any negative impact from the proposed change.

The licensee should also perform risk-informed evaluations of the proposed change to determine the impact on plant risk. The evaluation should explicitly consider the specific plant equipment affected by the proposed TS changes and the effects of the proposed change on the functionality,

¹This SRP adopts the 10 CFR Part 54 definition of current licensing basis. That is, "Current Licensing Basis (CLB) is the set of NRC requirements applicable to a specific plant and a licensee's written commitments for ensuring compliance with and operation with in applicable NRC requirements and the plant-specific design basis (including all modifications and additions to such commitments over the life of the license) that are docketed and in effect. The CLB includes the NRC regulations contained in 10 CFR Parts 2, 19, 20, 21, 26, 30, 40, 51, 54, 55, 70, 72, 73, 100 and appendices thereto; orders; license conditions; exemptions; and technical specifications. It also includes the plant-specific design-basis information defined in 10 CFR 50.2 as documented in the most recent final safety analysis report (FSAR) as required by 10 CFR 50.71 and the licensee's commitments remaining in effect that were made in docketed licensing correspondence such as licensee responses to NRC bulletins, generic letters, and enforcement actions, as well as licensee commitments documented in NRC safety evaluations or licensee event reports."

reliability, and availability of the affected equipment. The necessary scope and level of detail of the analysis depends upon the particular systems and functions that are affected, and it is recognized that there will be cases for which a qualitative, rather than quantitative, risk analysis is acceptable.

The licensee should provide the rationale that supports the acceptability of the proposed changes by integrating probabilistic insights with traditional considerations to arrive at final determination of risk. The determination should consider the continued conformance to existing applicable rules and regulations, the adequacy of the traditional engineering evaluation of the proposed change, and the change in plant risk relative to the acceptance guidelines. All of these areas should be adequately addressed before the change is considered acceptable. Section III.B provides a description of the review process for Element 2.

Element 3: Develop Implementation and Monitoring Program

The licensee should develop an implementation and performance monitoring program formulated to confirm the assumptions and analyses that were conducted to justify the CLB change, to ensure that plant operational safety can be maintained consistent with the assumptions in the PRA analysis of Element 2, and to ensure that the process provides criteria for taking actions based on the results of the monitoring efforts. Section III.C provides a description of the review process for Element 3.

Element 4: Submit Proposed Change

The final element involves the licensee's documentation of the analyses and submittal of the request. The submittal will be reviewed by NRC according to this standard review plan. Section III.D provides a description of the documentation guidelines for Element 4.

II. ACCEPTANCE GUIDELINES

For each TS application, the reviewers should ensure that each of the five key principles of the staff's philosophy of risk-informed decision making is met. These principles are described in Chapter 2 of Regulatory Guide DG-1065, "An Approach For Plant-Specific, Risk-Informed Decision Making: Technical Specifications." The following sections provide more specific guidelines on meeting these principles.

A. Traditional Engineering Guidelines

General traditional engineering acceptance guidelines can be found in SRP Chapter 19.0, Section II.3.1, "Evaluation of Defense-in-Depth Attributes and Safety Margins." Additional guidance as to how these acceptance guidelines relate to TS change requests is provided here.

1. Defense-in-Depth

The licensee should assess whether the proposed TS change meets the defense-in-depth principle (principle #2). Defense-in-depth consists of a number of elements as summarized below. These elements can be used as guidelines for making that assessment. Other equivalent acceptance guidelines are acceptable.

Defense-in-depth is maintained:

- a reasonable balance among prevention of core damage, prevention of containment failure, and consequence mitigation is preserved, e.g., the proposed change in a TS AOT or STI has not significantly changed the balance among these principles of prevention and mitigation. TS change requests should consider whether the anticipated operation changes associated with a change in an AOT or STI could introduce new accidents or transients or could increase the likelihood of an accident or transient.
- over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided, e.g., a programmatic configuration control process should not be relied upon to account for a large risk increase associated with a TS AOT extension.
- system redundancy, independence, and diversity are maintained commensurate with the expected frequency and consequences of challenges to the system, e.g., there are no risk outliers (the following items should be considered):
 - there are appropriate restrictions in place to preclude simultaneous equipment outages that would erode the principles of redundancy and diversity;

- compensatory actions to be taken when entering the extended AOT for pre-planned maintenance are identified;
 - voluntary removal of equipment from service during plant operation should not be scheduled when adverse weather conditions are predicted or at times when the plant may be subjected to other abnormal conditions;
 - the impact of the TS change on the safety function should be considered. For example, what is the impact of a change in the AOT for the low pressure safety injection system on the overall availability and reliability of the low pressure injection function?
- defenses against potential common cause failures are maintained and the potential for introduction of new common cause failure mechanisms is assessed, e.g., TS change requests should consider whether the anticipated operational changes associated with a change in an AOT or STI could introduce any new common cause failure modes not previously considered.
 - independence of barriers is not degraded, e.g., TS change requests should address the licensee's overall configuration risk management system which will provide a means of ensuring that the independence of barriers has not been degraded by the TS change.
 - defenses against human errors are maintained, e.g., TS change requests should consider whether the anticipated operation changes associated with a change in an AOT or STI could change the expected operator response or introduce any new human errors not previously considered.

2. Safety Margins

The engineering evaluation conducted should assess whether the impact of the proposed TS change is consistent with the principle that sufficient safety margins are maintained (principle #3). An acceptable set of guidelines for making that assessment are summarized below. Other equivalent decision guidelines are acceptable.

Sufficient safety margins are maintained:

- codes and standards or alternatives approved for use by the NRC are met, e.g., the proposed TS AOT or STI change is not in conflict with approved codes and standards relevant to the subject system.

- safety analysis acceptance criteria in the FSAR are met, or proposed revisions provide sufficient margin to account for analysis and data uncertainty, e.g., the proposed TS AOT or STI change does not adversely affect any assumptions or inputs to the safety analysis, or, if such inputs are affected, justification is provided to ensure sufficient safety margin will continue to exist. For TS AOT changes, an assessment should be made of the effect on the FSAR acceptance criteria assuming the plant is in the AOT (i.e., the subject equipment is inoperable), and there are no additional failures. Such an assessment should result in the identification of all situations where entry into the proposed AOT could result in failure to meet an intended safety function.
- 3. The licensee has demonstrated that the modification is needed and will ensure adequate reliability and availability of significant safety systems.
- 4. The licensee has provided the justification for the modification based on the guidance in Section III.A.

B. Probabilistic Guidelines

The guidelines discussed in Regulatory Guide DG-1061, Section 2.4.2, "Evaluation of Risk Impact, Including Treatment of Uncertainties" are applicable to TS change requests.

General guidelines for evaluating the risk impact from changes to the current licensing basis can be found in SRP Chapter 19.0, Section II.3.2, "Risk Assessment." It should be noted that these guidelines apply only to permanent changes to TS requirements. TS AOT changes are permanent changes, but, because AOTs are entered infrequently and are temporary by their very nature, the following additional guidelines are provided for TS AOT modifications:

1. The licensee has demonstrated that the TS AOT modification has only a very small quantitative impact on plant risk. An incremental conditional core damage probability (ICCDP)² of $5.0\text{E-}7$ is considered very small for a single TS AOT modification. Also, the ICCDP contribution should be distributed in time such that any increase in the associated instantaneous risk is very small and within the normal operating background (risk fluctuations) of the plant. A incremental conditional large early release probability (ICLERP) of $5.0\text{E-}8$ or less is also considered very small. (Tier 1)
2. The licensee has demonstrated that there are appropriate restrictions on dominant risk-significant configurations associated with the modification. (Tier 2)

²ICCDP = [(conditional CDF with the subject equipment out of service) - (baseline CDF with nominal expected equipment unavailabilities)] X (single AOT duration under consideration).

3. The licensee has implemented a risk-informed plant configuration control program. The licensee has implemented procedures to utilize, maintain, and control such a program.

In addition, if multiple TS changes are proposed, the cumulative impact of the proposed TS changes should be calculated and presented, in addition to the individual impacts. The total, cumulative impact should be estimated using the average value of the calculated risk metrics (e.g., CDF, LERF). The conditional measures (i.e., ICCDP and ICLERP) do not directly apply in evaluating the total impact from multiple changes.

In presenting the cumulative risk impact, the base case PRA model should be used consistently. It should not contain any of the proposed changes, but should reflect any other recent changes to the plant. The same model used for evaluating the individual changes should be used for assessing cumulative impact. Plant practices proposed for implementation as part of the TS changes should not be credited in the base case.

III. REVIEW PROCESS

Licensees are expected to provide strong technical bases for any TS change. The technical bases should be rooted in traditional engineering and system analyses. TS change requests based on PRA results alone should not be submitted for review. TS change requests should give proper attention to the integration of considerations such as conformance to Standard Technical Specifications, generic applicability of the requested change if it is different from Standard Technical Specifications, operational constraints, manufacturer recommendations, and practical considerations for test and maintenance. Standard practices used in setting AOTs and STIs should be followed, e.g., AOTs nominally used are 8 hours, 12 hours, 24 hours, 72 hours, 7 days, 14 days, etc. STIs nominally used are 12 hours, 7 days, 1 month, 3 months, etc. Using such standards greatly simplifies implementation, scheduling, monitoring, and auditing. Logical consistency among the requirements should be maintained, e.g., AOT requirements for multiple trains out of service should not be longer than that for one of the constituent trains.

A. **Definition of Proposed Change**

The licensee should include the reasons for requesting the TS change or changes in the submittal and should demonstrate the need for the requested change. Acceptable reasons for requesting TS modifications will most likely fall into one or more of the categories below.

1. **Improvement in Operational Safety**

The reason for TS modification may be to improve operational safety, that is, an improvement or reduction in the plant risk, or a reduction in occupational exposure of plant personnel in complying with the requirements.

2. **Consistency of Risk Basis in Regulatory Requirements**

The TS modifications requested can be supported by their risk implications. TS requirements can be changed to reflect improved design features in a plant or to reflect equipment reliability improvements that make a previous requirement unnecessarily stringent or ineffective. TS may be changed to establish consistently based requirements across the industry or across an industry group. It must be ensured that the risk following the change remains acceptable.

3. Reduce Unnecessary Burdens

The change may be needed to reduce unnecessary burdens in complying with current TS requirements, based on the operating history of the plant or industry in general. For example, in ~~specific instances~~, the usual repair time needed may be longer than the AOT defined in the TS. The required surveillance may lead to plant transients, result in unnecessary equipment wear, result in excessive radiation exposure to plant personnel, or place unnecessary administrative burdens on plant personnel that are not justified by the safety significance of the surveillance. In some cases, the change may provide operational flexibility, and in those cases, the change may increase the allocation of plant personnel's time to more safety-significant aspects of plant operation.

The reasons for requesting changes can form an important input in the decision to seek the requested changes and define the evaluations necessary to justify the modifications.

B. Engineering Evaluations

1. Traditional Engineering Evaluation

a. Compliance With Current Regulations

In evaluating proposed changes to TS, the licensee must ensure that current regulations are being followed (principle #1). The NRC regulations specific to TS requirements are stated in 10 CFR 50.36, "Technical Specifications." Additional information with regard to the NRC's policies on TS is contained in the NRC Final Policy Statement on Technical Specifications Improvements for Nuclear Power Reactors (58 FR 39132). These documents define the main elements of TS and provide criteria for items to be included in the TS. The final policy statement and the statement of consideration for 10 CFR 50.36 (60 FR 36953) also discuss the use of risk-informed approaches to improve TS. Regulations regarding application for and issuance of license amendments are found in 10 CFR 50.90, 50.91, and 50.92. In addition, the licensee should ensure that the TS change does not result in non-compliance with any other portion of the current licensing basis.

b. Evaluation of Defense-in-Depth Attributes & Safety Margins

One aspect of the engineering evaluations is to show that the fundamental safety principles on which the plant design was based are not compromised. Design basis accidents (DBAs) play a central role in nuclear power plant design. DBAs are a combination of postulated challenges and failure events against which plants are designed and design features that ensure adequate and safe plant response. During the design process, plant response and associated safety margins are evaluated using assumptions which are intended to be conservative. National standards and other

considerations such as defense-in-depth attributes and the single failure criterion constitute additional engineering considerations that influence plant design and operation. Margins and defenses associated with these considerations may be affected by the licensee's proposed TS change and, therefore, should be reevaluated to support a requested TS change. As part of this evaluation, the impact of the proposed TS change on affected equipment functionality, reliability, and availability will be determined. The engineering evaluation conducted should evaluate whether the impact of the proposed TS change is consistent with the principle that adequate defense-in-depth is maintained. In addition, the engineering evaluation conducted should assess whether the impact of the proposed TS change is consistent with the principle that adequate safety margins are maintained. The reviewers should confirm that the acceptance guidelines in Section II.A of this SRP are met with respect to the maintenance of defense-in-depth and safety margins.

c. Additional Engineering Considerations

Traditional engineering considerations that are unique to TS risk-informed techniques should also be taken into account in an engineering evaluation. These items can be summarized as follows:

- i. TS AOT and STI modifications should be supported by the overall safety benefit.
- ii. Justification for TS AOT modifications should be based on the need for extended equipment outage time and the demonstrated availability of redundant equipment. The AOT defined should be adequate to complete the majority of the component repairs or post-maintenance activities intended to be performed during power operation; however, AOTs should not be based solely on preventative maintenance activities that require long outage times but occur infrequently (e.g., once every five years). In addition, the AOT should be adequate to conduct any required surveillance tests that render the component or system inoperable. The burden of testing and maintenance can place a stress on the crew, which can affect the quality of the testing or maintenance and thereby the component reliability. Crew burden should be part of the consideration in deciding changes to requirements.
- iii. Regardless of the AOT, the actual time equipment is removed from service should be minimized. The removal should be performed during stable plant conditions and repeated TS entries should be avoided.
- iv. TS change requests should consider both plant-specific and industry-wide operational experience on systems important for coping with transients or accidents.
- v. Some systems may not be modeled by the plant's PRA but could affect the best estimate of

the performance or availability of systems that might provide a backup function for the system for which the TS change is being requested (this could change the required performance or availability of the system for which the TS change is being sought). The review should, therefore, consider systems beyond those modeled in the PRA.

2. Probabilistic Engineering Evaluation

The staff uses a three-tiered approach in its evaluation of the risk associated with proposed TS changes. The first tier is an evaluation of the impact on plant risk as expressed by the change in core damage frequency (Δ CDF), the incremental conditional core damage probability and the incremental conditional large early release probability resulting from the TS change. The second tier is an evaluation of the licensee's process used to address potentially high risk configurations that could exist if equipment in addition to that associated with the change were to be taken out of service simultaneously, or other risk significant operational factors such as concurrent system or equipment testing were also involved. The objective of this part of the staff's review is to ensure that appropriate restrictions on dominant risk-significant configurations associated with the change are in place. The third tier is an evaluation of the licensee's overall configuration risk management system to ensure that adequate programs and procedures are in place to identify and compensate for other potentially lower probability, but none the less risk significant, configurations resulting from maintenance and other operational activities.

a. Tier 1: PRA Capability and Insights

The first tier assesses the impact of the proposed TS modification on conditional core damage frequency (CCDF), incremental conditional core damage probability, and incremental conditional large early release probability. Two aspects need to be considered: 1) the validity of the PRA, and 2) the PRA insights and findings. The depth of the staff review at this stage will depend on the extent to which the licensee has demonstrated that its PRA is valid for assessing the proposed TS modifications and the overall impact of the TS change on plant risk. The key areas for review of Tier 1 considerations are discussed in the following sections.

I. Breadth and Depth of PRA Review

The breadth and depth of the PRA review should be addressed in the review for TS changes. The breadth and depth of the review will depend on several factors:

- a) The emphasis placed on traditional analysis as opposed to PRA in establishing the basis for the TS modification.

If the justification for the modification is based on well founded traditional arguments

that are easily supported by PRA insights, then only a limited PRA review may be warranted. However, if a TS change is primarily based on complex PRA arguments with a limited traditional basis, then the breadth and depth of the PRA review will be substantially greater.

- b) The safety significance of the structure, system or component under consideration.

The level of redundancy, diversity and need for operator recovery actions will impact the safety significance of any proposed TS modification. The reliance on operator actions to perform a safety function under high stress conditions will, for example, require greater scrutiny of the human reliability analysis than of automatic systems.

- c) The validity of the PRA.

An initial evaluation of the PRA will be needed to obtain a degree of confidence in the validity of the PRA. The necessary level of confidence will depend on the application. Validity of the PRA with respect to the decision making process can be established by evaluating:

- i) consistency of the PRA methodology with acceptable methods and practices
- ii) robustness of the results through sensitivity studies
- iii) consistency of the FRA findings with respect to the plant's design and operational characteristics
- iv) modeling detail and scope necessary to support the decision making activity
- v) representation of the as-built, as-operated plant

- d) The consistency of the TS modification to other TS proposals approved by the NRC.

If there is a baseline for approving similar TS modifications for similar type plants, then only differences between previously accepted submittals and the one under review would need to be assessed.

The need to independently validate the PRA in the context of the TS proposal is based on the need to establish a defensible probabilistic basis for approving the TS modification. The basis will depend on the extent to which PRA plays a role in the decision making process.

ii. PRA Review Considerations

The Tier 1 PRA review will cover the items presented below. Therefore the licensee's application must contain sufficient detail to evaluate these items. General guidance for reviewing these items

can be found in SRP Chapter 19.0, Section II.3.2, "Risk Assessment." Additional guidance specific to the review of TS modifications is provided here.

a) Quality of the PRA

The reviewer should consider the quality and validity of the PRA during the review of the licensee's submittal for the TS modification.

Has the PRA been previously reviewed by the NRC? Did the NRC SER on the IPE or other NRC reviews of the PRA identify any shortcomings? Have any identified shortcomings been addressed and satisfactorily resolved by the licensee, if they are relevant to the proposed TS modification?

Appendix X of Regulatory Guide DG-1061 and Section 4.3.1 of Regulatory Guide DG-1065 provides additional guidance on PRA quality.

b) Scope

A full scope PRA (Level 3) is not needed for TS evaluations. Also, in most cases, a Level 2 PRA with external events for all modes of operation will not be required for TS modification applications. If, for example, a system in question is only used at full power, no low-power or shutdown PRA is needed. The review of the scope of the PRA used in evaluating a TS modification should ensure that the guidance contained in Section 4.3.2 of Regulatory Guide DG-1065 is met.

c) Modeling Level of Detail

The review of the level of detail of the PRA used in evaluating a TS modification should ensure that the guidance contained in Section 4.4.3.1 of Regulatory Guide DG-1065 is met.

d) Modeling of Initiating Events

The review of initiating event modeling of the PRA used in evaluating a TS modification should ensure that the guidance contained in Section 4.3.3.2 of Regulatory Guide DG-1065 is met.

e) Screening Criteria and Truncation Limits

The review of the PRA screening criteria and truncation limits used in evaluating a TS modification should ensure that the guidance contained in Sections 4.3.3.3 and 4.3.3.4 of Regulatory Guide DG-1065 is met.

f) Assumptions in Applying PRA for TS Modifications

The review of the assumptions in applying the PRA to a TS modification should ensure that the guidance contained in Section 4.3.3.5 of Regulatory Guide DG-1065 is met.

g) PRA Assumptions

The review of the PRA assumptions used in evaluation a TS modification should ensure that the guidance contained in Section 4.3.4 of Regulatory Guide DG-1065 is met.

h) Sensitivity and Uncertainty Analyses

The review of any sensitivity and uncertainty analyses used in evaluating a TS modification should ensure that the guidance contained in Section 4.3.5 of Regulatory Guide DG-1065 is met.

b. Tier 2: Avoidance of Risk Significant Plant Configurations

The licensee's assessment should also provide reasonable assurance that risk-significant plant equipment outage configurations will not occur when specific plant equipment is out of service consistent with the proposed TS AOT modification. An effective way to perform such an assessment is to evaluate systems and/or components while in a LCO (equipment AOT) condition. Once system equipment is evaluated (by CCDF with LERF correlation), an assessment can be made as to whether certain enhancements to the TS, or procedures, are required to avoid risk-significant situations. In addition, compensatory actions that can mitigate any corresponding increase in risk, i.e., backup equipment, increased surveillance frequency, or upgrading procedures and training can be used to offset the risk associated with certain configurations. These compensatory actions should have been evaluated and incorporated into the first tier where practical to do so. In addition, the review of Tier 2 for TS modifications should ensure that the guidance contained in Section 4.3.6 of Regulatory Guide DG-1065 is met.

c. Tier 3: Risk Informed Plant Configuration Control/Management

The third tier focuses on licensee programs that ensure that the risk impact of out-of-service

equipment is appropriately evaluated prior to and while performing any maintenance activity. A viable program is able to uncover risk-significant plant equipment outage configurations as they evolve during normal plant operation. This can be accomplished by quantitatively evaluating the impact of equipment unavailability, operational activities like testing or load dispatching, or weather conditions on plant risk. The need for a third tier stems from the difficulty in identifying all possible risk-significant configurations under Tier 2. Tier 2 programs typically result in a table or set of tables that assume certain systems are unavailable and specify other systems that cannot be out of service under the assumed conditions. This third tier is needed because of the difficulty of providing a set of tables under Tier 2 that cover all plant configurations that will ever be encountered over extended periods of plant operation. In addition, the review of Tier 3 for TS modifications should ensure that the guidance contained in Section 4.3.7 of Regulatory Guide DG-1065 is met.

C. Implementation and Monitoring Program

Application of the three-tiered approach described below is in keeping with the fundamental principle that performance-based implementation and monitoring strategies be employed to account for uncertainties in analysis models and data (principle #5). Because of such uncertainties, these methods are used to avoid, or severely limit, the time durations during which plant operation is allowed with high-risk configurations of plant equipment (i.e., with excessive unavailability of critical safety equipment).

1. Three-Tiered Implementation Approach

As described in Section III.B.2 of this SRP, the staff has identified a three-tiered approach to evaluating the risk associated with proposed TS changes. The first tier is an evaluation of the impact on plant risk as expressed by the change in core damage frequency (Δ CDF), the incremental conditional core damage probability and the incremental conditional large early release probability resulting from the TS change. The second tier is an evaluation of the process used to address potentially high risk configurations that could exist if equipment in addition to that associated with the change were to be taken out of service simultaneously, or other risk significant operational factors such as concurrent system or equipment testing were also involved. The objective of this part of the review is to ensure that appropriate restrictions on dominant risk-significant configurations associated with the change are in place. The third tier is an evaluation of the overall configuration risk management system to ensure that adequate programs and procedures are in place to identify and compensate for other potentially lower probability, but none the less risk significant, configurations resulting from maintenance and other operational activities.

2. Maintenance Rule Control

In order to ensure that extension of a TS AOT or STI does not degrade operational safety over time, the licensee should ensure performance monitoring mechanisms are in place to identify negative trends in availability or reliability of equipment impacted by TS changes. As part of implementing the maintenance rule (10 CFR 50.65), each licensee most likely will have developed availability and reliability goals for the majority of TS equipment which could provide such a performance monitoring mechanism. The effect of TS changes should be considered if any adverse trends in meeting established goals are identified through implementation of the maintenance rule. If the licensee concludes that the performance or condition of a TS system or component affected by a TS change does not meet established goals, appropriate corrective action shall be taken to reverse the trend, in accordance with the maintenance rule. Such corrective action may include submittal of another TS change to shorten the revised AOT or STI, if the licensee determines this is an important factor in reversing the negative trend.

D. Documentation

The evaluations performed to justify the proposed TS changes should be documented and included in the license amendment request submittal. The documentation should include the following:

1. A description of the TS changes being proposed and the reasons for seeking the changes,
2. A description of the process used to arrive at the proposed changes,
3. Traditional engineering evaluations performed,
4. Changes made to the PRA for use in the TS change evaluation,
5. Review of the applicability and quality of the PRA models for TS evaluations,
6. Discussion of the risk measures used in the evaluating the changes,
7. Data additional to the plant's PRA database developed and used,
8. Summary of the risk measures calculated including intermediate results,

9. Sensitivity and uncertainty analyses performed,
10. Summary of the risk impacts of the proposed changes and any compensating actions proposed,
11. A tabulation of equipment outage configurations that could threaten the integrity of important safety functions and that are prohibited by TS or plant procedures (Tier 2).
12. A description of the capability to perform a contemporaneous assessment of the overall impact on safety of proposed plant configurations including an explanation of how these tools will be used to ensure that risk-significant plant configurations will not be entered and that appropriate actions will be taken when unforeseen events put the plant in a risk-significant configuration (Tier 3).
13. A marked up copy of the relevant TS and Bases. The level of detail provided in the TS Bases should include adequate information to provide the technical basis for the revised AOT or STI.
14. All other documentation required to be submitted with a license amendment request.

IV. EVALUATION FINDINGS

Refer to SRP Chapter 19.0, "Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decisionmaking: General Guidance," Section III, "Evaluation Findings," for guidance on this topic. In addition, the following items should be addressed in safety evaluations for TS changes.

- Background and NRC review objectives (Input from PRA Policy statement and other Commission documents).
- Breadth and depth of the review

The discussion of the breadth and depth of the review should consider the following factors:

- The emphasis placed on traditional analysis as opposed to PRA in establishing the basis for the TS modification.
- The safety significance of the structure, system or component under consideration.
- The validity of the PRA.
- The consistency of the TS modification to other TS proposals approved by the NRC.

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

VI. REFERENCES

1. Atomic Safety and Licensing Appeal Board, *Portland General Electric Company*. (Trojan Nuclear Plant), ALAB-531, 9 NRC 263 (1979).
2. *Codes of Federal Regulations*, Title 10, "Energy":
10 CFR 50.36, "Technical Specifications."
10 CFR 50.90 "Application for amendment of license or construction permit."
10 CFR 50.91 "Notice for public comment; State consultation."
10 CFR 50.92 "Issuance of amendment."
3. U.S. Nuclear Regulatory Commission, 33 FR 18612, Statement of Considerations, "Technical Specifications for Facility Licensees; Safety Analyses Reports," *Federal Register*, December 17, 1968.
4. U.S. Nuclear Regulatory Commission, 58 FR 39132, "Final Policy Statement on Technical Specifications Improvements for Nuclear Power Reactors," *Federal Register*, July 22, 1993
5. U.S. Nuclear Regulatory Commission, Final Rule, 10 CFR 50.36; 60 FR 36953, "Technical Specifications," *Federal Register*, July 19, 1995.
6. U.S. Nuclear Regulatory Commission Regulatory Guide DG-1065, An Approach For Plant-Specific, Risk-Informed Decision Making: Technical Specifications", December 1997.
7. NUREG-1430, "Standard Technical Specifications, Babcock and Wilcox Plants" (latest revision).
8. NUREG-1431, "Standard Technical Specifications, Westinghouse Plants" (latest revision).
9. NUREG-1432, "Standard Technical Specifications, Combustion Engineering Plants" (latest revision).
10. NUREG-1433, "Standard Technical Specifications, General Electric Plants, BWR/4" (latest revision).
11. NUREG-1434, "Standard Technical Specifications, General Electric Plants, BWR/6" (latest revision).

12. U.S. Nuclear Regulatory Commission, NUREG-CR-6141, "Handbook of Methods for Risk-Based Analyses of Technical Specifications," December 1994
13. Electric Power Research Institute TR-105867, "Guidelines for Preparing Risk-Based Technical Specifications Change Request Submittals," December 1995.
14. Electric Power Research Institute TR-105987, "Template for the Submission of Revised Risk-Based Technical Specifications," December 1995.
15. U.S. Nuclear Regulatory Commission Regulatory Guide DG-1061, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis," December 1997.
16. U.S. Nuclear Regulatory Commission, NUREG-0800, Chapter 19.0, "Standard Review Plan for Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decisionmaking: General Guidance," December 1997.

The Use of PRA in Risk-Informed Applications

Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

ABSTRACT

In August 1995, the Nuclear Regulatory Commission issued a policy statement proposing improved regulatory decisionmaking "by increasing the use of PRA [probabilistic risk assessment/analysis] in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data." To support the implementation of the Commission's policy, regulatory guidance documents have been developed by the staff (as drafts for public comment) describing how PRA can be used in specific regulatory activities, many of which relate to licensee-proposed changes to their current licensing basis (CLB). In addition, a more general regulatory guide has been developed which describes an overall approach to using PRA in risk-informed regulation. One key aspect of this general guidance is the attributes of an acceptable PRA for such regulatory activities. Detailed discussion is provided for a full-scope PRA (i.e., a PRA that considers both internal and external events for all modes of operation). In addition, discussions are provided for the use and limitations of importance measures and sensitivity studies. Finally, the subject of peer review of a PRA is also discussed.

CONTENTS

| | <u>Page</u> |
|--|-------------|
| ABSTRACT | iii |
| EXECUTIVE SUMMARY | xi |
| FOREWORD | xv |
| ACKNOWLEDGMENTS | xvii |
| ABBREVIATIONS | xviii |
| 1 INTRODUCTION | 1-1 |
| 1.1 Background | 1-1 |
| 1.2 Objectives | 1-2 |
| 1.3 Scope | 1-2 |
| 1.4 Role in Risk-Informed Regulation | 1-3 |
| 1.5 Report Organization | 1-4 |
| 2 INTERNAL EVENT LEVEL 1 PRA FOR FULL POWER OPERATIONS | 2-1 |
| 2.1 Internal Events Analysis | 2-1 |
| 2.1.1 Accident Sequence Initiating Event Analysis | 2-2 |
| 2.1.1.1 Considerations for the Baseline PRA | 2-2 |
| 2.1.1.2 Application Impact Considerations | 2-6 |
| 2.1.1.3 Interface with Other Tasks | 2-6 |
| 2.1.1.4 Documentation | 2-6 |
| 2.1.2 Accident Sequence Analysis | 2-7 |
| 2.1.2.1 Considerations for the Baseline PRA | 2-7 |
| 2.1.2.2 Application Impact Considerations | 2-12 |
| 2.1.2.3 Interfaces with Other Tasks | 2-12 |
| 2.1.2.4 Documentation | 2-13 |
| 2.1.3 Systems Analysis | 2-13 |
| 2.1.3.1 Considerations for the Baseline PRA | 2-13 |
| 2.1.3.2 Application Impact Considerations | 2-17 |
| 2.1.3.3 Interfaces with Other Tasks | 2-18 |
| 2.1.3.4 Documentation | 2-18 |
| 2.1.4 Data Analysis | 2-19 |
| 2.1.4.1 Considerations for the Baseline PRA | 2-19 |
| 2.1.4.2 Application Impact Considerations | 2-21 |
| 2.1.4.3 Interfaces with Other Tasks | 2-21 |
| 2.1.4.4 Documentation | 2-21 |
| 2.1.5 Human Reliability Analysis (HRA) | 2-22 |
| 2.1.5.1 Considerations for the Baseline HRA | 2-22 |
| 2.1.5.2 Application Impact Considerations | 2-27 |
| 2.1.5.3 Interfaces with Other Tasks | 2-27 |
| 2.1.5.4 Documentation | 2-28 |
| 2.1.6 Accident Sequence Quantification | 2-28 |
| 2.1.6.1 Considerations for the Baseline PRA | 2-28 |

CONTENTS (Cont'd)

| | <u>Page</u> |
|---|-------------|
| 2.1.6.2 Application Impact Considerations | 2-31 |
| 2.1.6.3 Interfaces with Other Tasks | 2-31 |
| 2.1.6.4 Documentation | 2-31 |
| 2.2 Internal Flooding Analysis | 2-32 |
| 2.2.1 Considerations for the Baseline PRA | 2-33 |
| 2.2.1.1 Identification and Screening of Flood Sources, Propagation Pathways, and Flood Scenarios | 2-33 |
| 2.2.1.2 Flooding Model Development and Quantification | 2-34 |
| 2.2.2 Application Impact Considerations | 2-34 |
| 2.2.3 Interface with Other Tasks | 2-35 |
| 2.2.4 Documentation | 2-35 |
| 2.3 Internal Fire Analysis | 2-35 |
| 2.3.1 Considerations for the Baseline PRA | 2-37 |
| 2.3.1.1 Defining Fire Areas of Fire Zones | 2-37 |
| 2.3.1.2 Equipment Identification and Mapping | 2-38 |
| 2.3.1.3 Fire Source Identification and Quantification | 2-38 |
| 2.3.1.4 Fire Growth and Spread Quantification | 2-39 |
| 2.3.1.5 Fire Damage Analysis | 2-39 |
| 2.3.1.6 Fire Detection and Suppression | 2-39 |
| 2.3.1.7 Human Intervention and Plant Recovery | 2-40 |
| 2.3.1.8 Fire Model Development and Quantification | 2-40 |
| 2.3.2 Application Impact Considerations | 2-43 |
| 2.3.3 Interface with Other Tasks | 2-43 |
| 2.3.4 Documentation | 2-43 |
| 3. INTERNAL EVENT LEVEL 2 PRA FOR FULL POWER OPERATIONS | 3-1 |
| 3.1 Evaluation of Containment Performance | 3-2 |
| 3.1.1 Assessment of Challenges to Containment Integrity | 3-2 |
| 3.1.1.1 Defining the Accident Sequences to be Assessed | 3-3 |
| 3.1.1.2 Assessment of Containment System Performance | 3-4 |
| 3.1.1.3 Evaluation of Severe Accident Progression | 3-6 |
| 3.1.2 Establishing Containment Performance Limits | 3-13 |
| 3.1.2.1 Considerations for the Baseline PRA | 3-14 |
| 3.1.2.2 Application Impact Considerations | 3-15 |
| 3.1.2.3 Interfaces with Other Tasks | 3-15 |
| 3.1.2.4 Documentation | 3-15 |
| 3.1.3 Probabilistic Modeling of Containment Performance | 3-16 |
| 3.1.3.1 Considerations for the Baseline PRA | 3-16 |
| 3.1.3.2 Application Impact Considerations | 3-18 |
| 3.1.3.3 Interfaces with Other Tasks | 3-19 |
| 3.1.3.4 Documentation | 3-19 |
| 3.2 Radionuclide Release Characterization | 3-19 |
| 3.2.1 Definition of Radionuclide Source Terms | 3-20 |
| 3.2.1.1 Considerations for the Baseline PRA | 3-20 |

CONTENTS (Cont'd)

| | <u>Page</u> |
|---|-------------|
| 3.2.1.2 Application Impact Considerations | 3-21 |
| 3.2.1.3 Interfaces with Other Tasks | 3-21 |
| 3.2.1.4 Documentation | 3-21 |
| 3.2.2 Coupling Source Term and Severe Accident Progression Analyses | 3-22 |
| 3.2.2.1 Considerations for the Baseline PRA | 3-22 |
| 3.2.2.2 Application Impact Considerations | 3-23 |
| 3.2.2.3 Interfaces with Other Tasks | 3-23 |
| 3.2.2.4 Documentation | 3-23 |
| 3.2.3 Treatment of Source Term Uncertainties | 3-23 |
| 3.2.3.1 Considerations for the Baseline PRA | 3-24 |
| 3.2.3.2 Application Impact Considerations | 3-24 |
| 3.2.3.3 Interfaces with Other Tasks | 3-24 |
| 3.2.3.4 Documentation | 3-25 |
| 4 INTERNAL EVENT LEVEL 3 PRA FOR FULL POWER OPERATIONS | 4-1 |
| 4.1 Accident Consequence Analysis | 4-1 |
| 4.1.1 Considerations for the Baseline PRA | 4-2 |
| 4.1.2 Application Impact Considerations | 4-2 |
| 4.1.3 Interfaces with Other Tasks | 4-3 |
| 4.1.4 Documentation | 4-3 |
| 4.2 Computation of Risk | 4-3 |
| 4.2.1 Considerations for the Baseline PRA | 4-3 |
| 4.2.2 Application Impact Considerations | 4-3 |
| 4.2.3 Interfaces with Other Tasks | 4-3 |
| 4.2.4 Documentation | 4-4 |
| 5 EXTERNAL EVENT PRA FOR FULL POWER OPERATION | 5-1 |
| 5.1 Level 1 Analysis | 5-1 |
| 5.1.1 Seismic Analysis | 5-1 |
| 5.1.1.1 Considerations for the Baseline PRA | 5-1 |
| 5.1.1.2 Application Impact Considerations | 5-4 |
| 5.1.1.3 Interfaces with Other Tasks | 5-4 |
| 5.1.1.4 Documentation | 5-4 |
| 5.1.2 Analysis of "Other" External Events | 5-6 |
| 5.1.2.1 Considerations for the Baseline PRA | 5-6 |
| 5.1.2.2 Application Impact Considerations | 5-6 |
| 5.1.2.3 Interfaces with Other Tasks | 5-7 |
| 5.1.2.4 Documentation | 5-7 |
| 5.2 Level 2 Analysis | 5-7 |
| 5.2.1 Seismic Analysis | 5-7 |
| 5.2.2 Analysis of "Other" External Events | 5-8 |

CONTENTS (Cont'd)

| | <u>Page</u> |
|---|-------------|
| 5.3 Level 3 Analysis | 5-8 |
| 5.3.1 Seismic Analysis | 5-8 |
| 5.3.2 Analysis of "Other" External Events | 5-8 |
| 6. INTERNAL AND EXTERNAL EVENT PRA FOR LOW POWER AND SHUTDOWN OPERATIONS | 6-1 |
| 6.1 Internal Events Level 1 Analysis | 6-2 |
| 6.1.1 Plant Operational States | 6-2 |
| 6.1.1.1 Consideration for the Baseline PRA | 6 |
| 6.1.1.2 Application Impact Considerations | 6-3 |
| 6.1.1.3 Interfaces with Other Tasks | 6-3 |
| 6.1.1.4 Documentation | 6-3 |
| 6.1.2 Accident Sequence Initiating Event Analysis | 6-4 |
| 6.1.3 Accident Sequence Analysis | 6-5 |
| 6.1.4 Systems Analysis | 6-6 |
| 6.1.5 Data Analysis | 6-6 |
| 6.1.6 Human Reliability Analysis (HRA) | 6-7 |
| 6.1.7 Accident Sequence Quantification | 6-7 |
| 6.2 Internal Flood Level 1 Analysis | 6-7 |
| 6.2.1 Definition and Characterization of Plant Operational States | 6-7 |
| 6.2.2 Initiating Event Analysis | 6-7 |
| 6.2.3 Flood Propagation | 6-8 |
| 6.2.4 Flood Model Development and Quantification | 6-8 |
| 6.3 Internal Fire Level 1 Analysis | 6-8 |
| 6.3.1 Definition and Characterization of Plant Operational States | 6-9 |
| 6.3.2 Initiating Event Analysis | 6-9 |
| 6.3.3 Identification of Critical Fire Locations | 6-9 |
| 6.3.4 Fire Propagation and Suppression | 6-9 |
| 6.3.5 Fire Model Development and Quantification | 6-9 |
| 6.4 Seismic Level 1 Analysis | 6-10 |
| 6.4.1 Definition and Characterization of Plant Operational States | 6-10 |
| 6.4.2 Initiating Event Analysis | 6-10 |
| 6.4.3 Identification of Structures, Systems, and Components (SSCs) | 6-10 |
| 6.4.4 Hazard Analysis | 6-10 |
| 6.4.5 Fragility Analysis | 6-10 |
| 6.4.6 Model Development and Quantification | 6-11 |
| 6.5 Level 1 Analysis of "Other" External Events | 6-11 |
| 6.6 Level 2 Analysis | 6-11 |
| 6.6.1 Considerations for the Baseline PRA | 6-12 |
| 6.6.2 Application Impact Considerations | 6-12 |
| 6.6.3 Interfaces with Other Tasks | 6-12 |
| 6.6.4 Documentation | 6-12 |
| 6.7 Level 3 Analysis | 6-13 |

CONTENTS (Cont'd)

| | <u>Page</u> |
|--|-------------|
| APPENDIX A. PRIORITIZATION OF SSCS AND HUMAN ACTIONS | A-1 |
| A.1 Introduction and Objective | A-1 |
| A.2 PRA-Based Importance Assessment | A-2 |
| A.2.1 Quantitative Importance Measures | A-2 |
| A.2.1.1 Definitions of Importance Measures | A-2 |
| A.2.1.2 Considerations in Calculating Importance Measures | A-4 |
| A.2.2 Qualitative importance Measures | A-7 |
| A.2.3 Considerations for Ranking Using Importance Measures | A-8 |
| A.3 Safety-Based Prioritization | A-11 |
| A.4 Integration | A-13 |
| APPENDIX B. PRA PEER REVIEW | B-1 |
| B.1 Objectives of the Review | B-1 |
| B.2 Review Team Composition and Qualifications | B-1 |
| B.3 Review Process and Considerations | B-2 |
| B.4 Documentation of Findings | B-6 |

EXECUTIVE SUMMARY

Introduction

In August 1995, the Nuclear Regulatory Commission (NRC) issued a policy statement proposing improved regulatory decisionmaking "by increasing the use of PRA [probabilistic risk assessment/analysis] in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data." To support the implementation of the Commission's policy, regulatory guidance documents are being developed by the staff (currently as drafts for public comment) describing how PRA can be used in specific regulatory activities, many of which relate to licensee-proposed changes to their current licensing basis (CLB). One key aspect of using PRA for such regulatory activities is what are the appropriate scope and attributes of the PRA. The main purpose of this report is to address the scope and attributes of a PRA that adequately represents the plant design and operation. It is recognized that the scope and attributes of a PRA may be different depending upon its intended use or on the issue being evaluated. Accordingly, this report is intended for use as reference or supporting information which PRA analysts can use to help in making decisions regarding the scope and attributes of a PRA appropriate for their analysis. Thus, this report can be used to help:

- Define the main attributes of each task of a PRA that is intended to support risk-informed regulatory decisionmaking.
- Identify task-by-task issues that should be considered when using a PRA to assess the impact of proposed CLB changes.
- Provide supporting information for peer reviewers judging the adequacy of a PRA intended to support risk-informed decisionmaking, and
- Identify attributes and limitations of importance analyses and qualitative ranking methods that are most appropriate for use in screening analyses and in categorization of structures, systems, and components (SSCs) and human activities according to their contribution to risk and safety.

In addition, this report may be a valuable step in the development of standards for PRAs. As discussed in OMB Circular No. A-119 (FRN, Vol. 58, No. 205, October 26, 1993), federal agencies have been directed to make greater use of consensus standards in their activities. As such, the staff will be interacting with technical societies and others to develop such consensus standards in parallel with the finalization of this report.

Scope and Limitations

A PRA of a nuclear power plant is an analytical process that quantifies the potential risk associated with the design, operation and maintenance of the plant to the health and safety of the public. Traditionally, a full-scope PRA is used to quantify the risk from accidents initiated in the plant (from internal initiating events such as pipe breaks and external initiating events such as earthquakes) and during both full power and low power/shutdown conditions.

The risk evaluation involves three sequential parts or "levels": identification and quantification of the sequences of events leading to core damage (Level 1 analysis); evaluation and quantification of the mechanisms, amounts, and probabilities of subsequent radioactive material releases from the containment (Level 2 analysis); and the evaluation and quantification of the resulting consequences to both the public and the environment (Level 3 analysis). A full-scope PRA, as defined here, does not include evaluation of accidents initiated by sabotage events or that result in

releases from other radioactive material sources such as the spent fuel pool, routine, small releases of radioactive material, and does not include the risk to plant personnel from any accident.

The elements of a full-scope PRA, and the attributes for the analysis of each element, presented in this report reflect the following general considerations:

- The design, construction, and operational practices of the plant being analyzed is expected to be consistent with its CLB.
- The PRA being performed is expected to realistically reflect the design, construction, and operational practices. The Commission's policy statement on the expanded use of PRA indicates that "PRA evaluations in support of regulatory decisions should be as realistic as practicable." Consequently, the PRA used to support risk-informed decisionmaking is expected to reflect the impact of previous changes made to the CLB. In this context, it is presumed that the particular application of PRA for which these attributes apply is quantitative in nature, and that the change under consideration can be modeled in the PRA (by manipulation of basic event information or the event tree/fault tree logic model).
- The discussions presented in the report are in terms of functional requirements. In general, prescriptive guidance is not provided, nor are characterizations of specific methods. In some circumstances, however, where an issue is both important to risk results and poorly understood, prescriptive solutions are stated to reduce potential PRA-to-PRA variability.
- The described PRA attributes are meant to cover a wide range of risk-informed regulatory applications. Additional attributes for specific applications are described in the application-specific regulatory guides.
- PRA models have been developed and are being used for real-time monitoring of plant operations (and resulting monitoring of risks). The attributes for such models may be quite different from those for models associated with regulatory applications, and are, therefore, not addressed in this report.

Role in Risk-Informed Regulation

This document discusses PRA attributes that support Draft Regulatory Guide DG-1061, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to Current Licensing Basis," and the Draft Standard Review Plan (Chapter 19), "Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decisionmaking: General Guidance." This report also is referenced by related risk-informed regulatory guides and their corresponding standard review plan chapters. These include DG-1062 on inservice testing, DG-1063 on inservice inspection of piping, DG-1064 on graded quality assurance, and DG-1065 on technical specifications.

As mentioned above, the content of this report is meant to support a wide variety of risk-informed applications that may exceed those covered in the staff's PRA implementation plan. Each risk-informed application imposes different requirements on the supporting PRA scope and level of detail. This document is intended to be flexible to accommodate and benefit these applications. Some applications are complex and may necessitate a higher standard and high accuracy from a supporting PRA. Since these applications are the most demanding, they dictate the level of technical detail in this document. However, less demanding applications, such as those that need information only about PRA insights, or those that rely on quantitative results only in selected areas of the PRA, may use, as appropriate, simpler models as compared to those described in this document. The process for using risk information in regulatory decisionmaking starts with definition of the scope of the particular application under consideration. This

information should be used to identify areas (tasks) in the supporting PRA that are influenced by the application and the type of support information needed. This information, in turn, can be used to define applicable portions of this report. Application-specific regulatory guides include further guidance in this area.

- Has sufficient supporting information for peer reviewers judging the adequacy of a PRA intended to support risk-informed decisionmaking been provided?
- Have the attributes and limitations of importance analyses and qualitative ranking methods that are most appropriate for use in screening analyses and in categorization of structures, systems, and components (SSCs) and human activities according to their contribution to risk and safety been adequately discussed?
- Is this report a useful step towards development of consensus standards for PRA methods? What steps should be next taken?

All comments should be addressed in writing within 90 days to:

Mark Cunningham
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
MS T10E50
Washington, DC 20555

This report will be issued in final form after it is revised on the basis of comments received.

M. Wayne Hodges, Director
Division of Systems Technology
Office of Nuclear Regulatory Research

FOREWORD

During the last several years, both the U.S. Nuclear Regulatory Commission (NRC) and the nuclear industry have recognized that probabilistic risk assessment (PRA) has evolved to the point where it can be used increasingly as a tool in regulatory decisionmaking. In August 1995, the NRC adopted the following policy statement regarding the expanded NRC use of PRA.

- The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.
- PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices. Where appropriate, PRA should be used to support the proposal of additional regulatory requirements in accordance with 10 CFR 50.109. Appropriate procedures for including PRA in the process for changing regulatory requirements should be developed and followed. It is, of course, understood that the intent of this policy is that existing rules and regulations will be complied with unless these rules and regulations are revised.
- PRA evaluations in support of regulatory decisions should be as realistic as practicable and appropriate supporting data should be publicly available for review.
- The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgements on the need for proposing and backfitting new generic requirements on nuclear power plant licensees.

In its approval of the policy statement, the Commission articulated its expectation that implementation of the policy statement will improve the regulatory process in three areas: foremost, through safety decisionmaking enhanced by the use of PRA insights; through more efficient use of agency resources; and through a reduction in unnecessary burden on licensees. In parallel with the publication of the policy statement, the staff developed an implementation plan to define and organize the PRA-related activities being undertaken. These activities cover a wide range of PRA applications and involve the use of a variety of PRA methods (with variety including both types of models used and the detail of modeling needed). This report focuses on defining the attributes of a PRA that will enable it to support a variety of applications described in the staff PRA implementation plan. These applications vary in complexity and hence the demand on the quality of the supporting PRA will also vary. While reading and reviewing this draft report, the reader should keep in mind that the level of detail and model complexity are influenced by the issue being analyzed.

This report is issued as a draft for comment. Specifically, comments on the following questions are requested:

- Have the main attributes of each task of a PRA intended to support risk-informed regulatory decisionmaking been defined?
- Have task-by-task issues that should be considered when using a PRA to assess the impact of proposed current licensing basis changes been defined?

ACKNOWLEDGMENTS

This report is the result of committed, creative, and professional efforts by the NRC staff and contractors.

Overall leadership of the project was provided by:

Ann Ramey-Smith, NRC

The principal authors of this report, in alphabetical order, are:

Ali Azarm, Brookhaven National Laboratory (BNL)

Allen Camp, Sandia National Laboratories (SNL)

Susan Dingman, SNL

Mary Drouin, NRC

Adel El-Bassioni, NRC

Alan Kolaczowski, Science Applications
International Corporation (SAIC)

Jeff LaChance (SAIC)

Mark Leonard, Innovative Technology Solutions

Trevor Pratt, BNL

Donnie Whitehead, SNL

Other contributors include:

Bennett Brady, NRC

Thomas Brown, SNL

Tsong-Lun Chu, BNL

Julie Gregory, SNL

Jack Guttmann, NRC

Brad Hardin, NRC

Vinod Mubayi, BNL

Hossein Nourbakhsh, BNL

Nathan Siu, INEL

Roy Woods, NRC

Primary reviewers include:

Patrick Baranowsky, NRC

Rudolph Bernard, NRC

Michael Cheok, NRC

Mark Cunningham, NRC

Stephen Dinsmore, NRC

Wayne Hodges, NRC

Thomas King, NRC

Joseph Murphy, NRC

Gareth Parry, NRC

Dale Rasmuson, NRC

Administrative support:

Mahmooda Bano, NRC

Alice Costantini, BNL

Wendy Eisenberg, NRC

Jean Frejka, BNL

Barbara Jordon, NRC

Emily Preston, SNL

Donna Storan, BNL

ABBREVIATIONS

| | |
|-------------|---|
| AC | Alternating Current |
| ADS | Automatic Depressurization System |
| AEOD | Office of Analysis and Evaluation of Operational Data |
| ALARA | As Low as Reasonably Achievable |
| ASME | American Society of Mechanical Engineers |
| ATWS | Anticipated Transient Without Scram |
| BM | Birnbaum Measure |
| BWR | Boiling Water Reactor |
| CCF | Common Cause Failure |
| CCFP | Conditional Containment Failure Probability |
| CCI | Core-Concrete Interactions |
| CDF | Core Damage Frequency |
| CLB | Current Licensing Basis |
| CRAC | Calculations of Reactor Accident Consequences |
| CRD | Control Rod Drive |
| DC | Direct Current |
| DCH | Direct Containment Heating |
| DDT | Deflagration to Detonation Transition |
| DOE | Department of Energy |
| ECCS | Emergency Core Cooling System |
| EOPs | Emergency Operating Procedures |
| EPRI | Electric Power Research Institute |
| FCI | Fuel Coolant Interaction |
| FIVE | Fire Induced Vulnerability Evaluation |
| FMEA | Failure Modes and Effects Analysis |
| FSAR | Final Safety Analysis Report |
| FV | Fussell-Vesely |
| GL | Generic Letter |
| HCLPF | High-Confidence-and-Low-Probability |
| HEP | Human Error Probability |
| HPCI | High-Pressure Coolant Injection |
| HRA | Human Reliability Analysis |
| HSSCs/LSSCs | High and Low Safety Significant Components |
| HVAC | Heating, Ventilation, and Air Conditioning |
| IPE | Individual Plant Examination |
| IPEEE | Individual Plant Examination of External Events |
| ISI | In-service Inspection |
| ISLOCA | Interfacing System Loss-of-Coolant Accident |
| IST | In-service Testing |
| kV | Kilovolt |
| LER | Licensee Event Report |
| LERF | Large Early Release Frequency |
| LLNL | Lawrence Livermore National Laboratory |

ABBREVIATIONS (Cont'd)

| | |
|-------|---|
| LOCA | Loss-of-Coolant Accident |
| LOOP | Loss of Offsite Power |
| LP&S | Low Power and Shutdown |
| LPCI | Low-Pressure Coolant Injection |
| MAAP | Modular Accident Analysis Program |
| MACCS | MELCOR Accident Consequence Code System |
| MCR | Minimal Cutset Ranking |
| MOV | Motor-Operated Valve |
| MPR | Minimal Pathset Ranking |
| MTC | Moderator Temperature Coefficient |
| NPSH | Net Positive Suction Head |
| NRC | Nuclear Regulatory Commission |
| NSSS | Nuclear Steam Supply System |
| PCA | Probabilistic Consequence Assessment |
| PCS | Power Conversion System |
| PDS | Plant Damage State |
| POS | Plant Operational State |
| PRA | Probabilistic Risk Assessment/Analysis |
| PSF | Performance Shaping Factor |
| PWR | Pressurized Water Reactor |
| QA | Quality Assurance |
| QRR | Qualitative Risk Ranking |
| RAW | Risk Achievement Worth |
| RCIC | Reactor Core Isolation Cooling |
| RCP | Reactor Coolant Pump |
| RCS | Reactor Coolant System |
| RHR | Residual Heat Removal |
| RIR | Risk Informed Regulation |
| RPS | Reactor Protection System |
| RPT | Recirculation Pump Trip |
| RPV | Reactor Pressure Vessel |
| RRW | Risk Reduction Worth |
| RWST | Refueling Water Storage Tank |
| SAR | Safety Analysis Report |
| SBO | Station Blackout |
| SERG | Steam Explosion Review Group |
| SG | Steam Generator |
| SGTR | Steam Generator Tube Rupture |
| SLC | Standby Liquid Control |
| SRV | Safety Relief Valve |
| SSCs | Structures, Systems, and Components |
| THERP | Technique for Human Error Rate Prediction |
| TS | Technical Specifications |
| U.S. | United States |

1. INTRODUCTION

1.1 Background

During the last several years, both the U.S. Nuclear Regulatory Commission (NRC) and the nuclear industry have recognized that probabilistic risk assessment (PRA) has evolved to the point where it can be used increasingly as a tool in regulatory decisionmaking. In August 1995, the NRC adopted the following policy statement regarding the expanded NRC use of PRA.

- The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.
- PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments and staff practices. Where appropriate, PRA should be used to support the proposal of additional regulatory requirements in accordance with 10 CFR 50.109 (Ref. 1.1). Appropriate procedures for including PRA in the process for changing regulatory requirements should be developed and followed. It is, of course, understood that the intent of this policy is that existing rules and regulations will be complied with unless these rules and regulations are revised.
- PRA evaluations in support of regulatory decisions should be as realistic as practicable and appropriate supporting data should be publicly available for review.
- The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgments on the need for proposing and backfitting new generic requirements on nuclear power plant licensees.

In its approval of the policy statement, the Commission articulated its expectation that implementation of the policy statement will improve the regulatory process in three areas: foremost, through safety decisionmaking enhanced by the use of PRA insights; through more efficient use of agency resources; and through a reduction in unnecessary burdens on licensees. In parallel with the publication of the policy statement, the staff developed an implementation plan to define and organize the PRA-related activities being undertaken. These activities cover a wide range of PRA applications and involve the use of a variety of PRA methods (with variety including both types of models used and the detail of modeling needed). For example, one application involves the use of PRA in the assessment of operational events in reactors. The characteristics of these assessments dictates that relatively simple PRA models be used. In contrast, other applications may necessitate the use of detailed models.

This report focuses on defining the attributes of a PRA that enable it to support a variety of applications described in the staff PRA implementation plan. These applications vary in complexity and hence the demand on the quality of the supporting PRA will also vary. While reading and reviewing this report, the reader should keep in mind that the described level of detail and model complexity are focussed on those risk-informed applications that are most demanding as far as PRA quality is concerned. Allowance for less demanding risk-informed applications is acceptable provided it is properly justified. In addition, discussion is also provided to direct the PRA user to those attributes in each PRA task that may be impacted by risk-informed applications.

1 Introduction

As discussed in OMB Circular No. A-119 (FRN, Vol. 58, No. 205, October 26, 1993), federal agencies have been directed to make greater use of consensus standards in their activities. This report may be a first step in the development of standards for PRAs. As such, the staff will be interacting with technical societies and others to develop such consensus standards in parallel with the finalization of this report.

1.2 Objectives

This report can be used to help:

1. Define the main attributes of each task of a state-of-the-art PRA that is intended to support risk-informed regulatory decisionmaking.
2. Identify task-by-task issues that should be considered when using a PRA to assess the impact of proposed current licensing basis (CLB) changes.
3. Provide supporting information for peer reviewers judging the adequacy of a PRA intended to support risk-informed decisionmaking.
4. Discuss attributes and the limitations of importance analyses and qualitative ranking methods that are most appropriate for use in screening analyses and in categorization of structures, systems, and components (SSCs) and human activities according to their contribution to risk and safety.

In addition, staff regards the content of this report as a first step towards the development of consensus standards of PRAs.

1.3 Scope

A PRA of a nuclear power plant is an analytical process that quantifies the potential risk associated with the design, operation and maintenance of the plant to the health and safety of the public. Traditionally, a full-scope PRA is used to quantify the risk from accidents initiated in the plant (from internal initiating events such as pipe breaks and external initiating events such as earthquakes) and during both full power and low power/shutdown conditions.

The risk evaluation involves three sequential parts or "levels": identification and quantification of the sequences of events leading to core damage (Level 1 analysis); evaluation and quantification of the mechanisms, amounts, and probabilities of subsequent radioactive material releases from the containment (Level 2 analysis); and the evaluation and quantification of the resulting consequences to both the public and the environment (Level 3 analysis). A full-scope PRA, as defined here, does not include evaluation of accidents initiated by sabotage events or that result in releases from other radioactive material sources such as the spent fuel pool, routine, small releases of radioactive material, and does not include the risk to plant personnel from any accident.

The elements of a full-scope PRA, and the attributes for the analysis of each element, are presented in the following sections. While reading and reviewing this report, the reader should keep in mind the following general considerations:

- The design, construction, and operational practices of the plant being analyzed is expected to be consistent with its CLB.

- The PRA being performed is expected to realistically reflect the design, construction, and operational practices. The Commission's policy statement indicates that "PRA evaluations in support of regulatory decisions should be as realistic as practicable." Consequently, the PRA used to support risk-informed decisionmaking is expected to reflect the impact of previous changes made to the CLB. In this context, it is presumed that the particular application of PRA for which these attributes apply is quantitative in nature, and that the change under consideration can be modeled in the PRA (by manipulation of basic event information or the event tree/fault tree logic model).
- This document is not a procedures guide for performing a PRA. Such procedures are available in numerous documents including NUREG/CR-2300, NUREG/CR-2815, NUREG/CR-2728, NUREG/CR-4550, Volume 1, NUREG/CR-4840, and NUREG/CR-5259 (Ref. 1.2). This document provides attributes (for each PRA task) against which a PRA study and its supporting documentation can be compared, then modified and/or supplemented as needed.
- The discussions described below are provided in terms of functional requirements. In general, prescriptive guidance is not provided, nor are characterizations of specific methods. In some circumstances, however, where an issue is both important to risk results and poorly understood, prescriptive solutions are purposely provided to reduce PRA-to-PRA variability.
- The described PRA attributes are meant to cover the most demanding risk-informed regulatory applications, although the principal focus for this draft version of the document has been uses of PRA in CLB changes. Additional attributes for specific applications are described in the application-specific regulatory guides.
- PRA models have been developed and are being used for real-time monitoring of plant operations (and resulting monitoring of risks). The attributes for such models may be quite different from those for models associated with regulatory applications, and are not addressed here.

1.4 Role in Risk-Informed Regulation

This document discusses PRA attributes that support Draft Regulatory Guide DG-1061, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to Current Licensing Basis," and the Draft Standard Review Plan (Chapter 19), "Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decisionmaking: General Guidance." This report also is referenced by related risk-informed regulatory guides and their corresponding standard review plan chapters. These include DG-1062 on inservice testing, DG-1063 on inservice inspection of piping, DG-1064 on graded quality assurance, and DG-1065 on technical specifications (Ref. 1.3).

As mentioned above, the content in this report is meant to support a wide variety of risk-informed applications that may exceed those covered in the staff's PRA implementation plan. Each risk-informed application imposes different requirements on the supporting PRA scope and level of detail. This document is intended to be flexible to accommodate and benefit these applications. Some applications are complex and may necessitate a higher standard and high accuracy from a supporting PRA. Since these applications are the most demanding, they dictate the level of technical detail in this document. However, less demanding applications, such as those that need information only about PRA insights, or those that rely on quantitative results only in selected areas of the PRA, may use, as appropriate, simpler models as compared to those described in this document. The process for using risk information in regulatory decisionmaking starts with definition of the scope of the particular application under consideration. This

1 Introduction

information should be used to identify areas (tasks) in the supporting PRA that are influenced by the application, and the type of support information needed. This information, in turn, can be used to define applicable portions of this report. Application-specific regulatory guides include further guidance in this area.

1.5 Report Organization

Most PRAs performed for U.S. nuclear power plants have focused on accidents initiated by internal events (including internal floods and fires) during full power operations. As such, the attributes for a PRA applicable to a power plant during full power operations are described in Chapters 2 through 4, and in significant detail. Chapter 2 provides the attributes of a Level 1 PRA with emphasis on accidents initiated by internal events. Chapter 3 follows a similar format to Chapter 2 but for a Level 2 PRA. Attributes of a Level 3 PRA are presented in Chapter 4. Accidents initiated by external events during full power operation are addressed in Chapter 5, which considers all the levels of analysis. In Chapter 6, the attributes of a PRA for low power and shutdown operations are presented. Chapter 6 includes consideration of accidents initiated by internal and external events and for all three levels of analysis. Information on the use and limitations of importance measures is provided in Appendix A. Finally, Appendix B presents information for peer reviews of a PRA.

REFERENCES FOR CHAPTER 1

- 1.1. USNRC, "Backfitting," Code of Federal Regulation, Title 10, Section 50.109, Amended April 18, 1989.
- 1.2. "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," NUREG/CR-2300, Vols. 1 and 2, American Nuclear Society and Institute of Electrical and Electronic Engineers, January 1983.
- R. A. Bari, et al., "Probabilistic Safety Analysis Procedures Guide," NUREG/CR-2815, BNL-NUREG-51559, Vols. 1 and 2, Revision 1, Brookhaven National Laboratory, August 1985.
- D. D. Carlson, "Interim Reliability Evaluation Program Procedures Guide," NUREG/CR-2728, SAND82-1100, Sandia National Laboratories, January 1983.
- D. M. Ericson, Jr. (editor), et al., "Analysis of Core Damage Frequency: Internal Events Methodology," NUREG/CR-4550, SAND86-2084, Volume 1, Revision 1, Sandia National Laboratories, January 1990.
- M. P. Bohn and J. A. Lambright, "Procedures for the External Event Core Damage Frequency Analysis for NUREG-1150," NUREG/CR-4840, Sandia National Laboratories, November 1990.
- "Individual Plant Examination for External Events: Guidance and Procedures," NUREG/CR-5259, Draft, March 1989.
- 1.3. USNRC, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis," Draft Regulatory Guide DG-1061, February 1997.
- USNRC, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Inservice Testing," Draft Regulatory Guide DG-1062, February 1997.
- USNRC, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Inservice Inspection," Draft Regulatory Guide DG-1063, February 1997.
- USNRC, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Graded Quality Assurance," Draft Regulatory Guide DG-1064, February 1997.
- USNRC, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications," Draft Regulatory Guide DG-1065, February 1997.

2. INTERNAL EVENT LEVEL 1 PRA FOR FULL POWER OPERATIONS

This chapter provides attributes for a Level 1 probabilistic risk assessment (PRA) of a power plant for accidents initiated during full power operations. Full power is defined to encompass the operations that occur while the plant is at greater than 15% of rated power. A Level 1 PRA identifies and quantifies those accident sequences that could lead to the onset of core damage. A summation of all such accidents leads to an estimate of the core damage frequency (CDF). Accidents initiated by internal events are discussed in the following section. Accidents initiated by various external events are addressed in Chapter 5.

2.1 Internal Events Analysis

This section provides the attributes for performing a Level 1 PRA for analysis of internal events at full power operation. The attributes are also generally applicable to the analysis of external events at full power and for the analysis of all events during low-power and shutdown conditions. Additional attributes applicable only to the analysis of external events are provided in Chapter 5. Additional attributes unique to the analysis of the risk from low-power and shutdown operations are presented in Chapter 6.

A Level 1 PRA is comprised of three major segments:

- The identification of those sequences of events that, if not prevented, could result in a core damage state and the potential release of radionuclides.
- The development of models of events that contribute to the core damage sequences.
- The quantification of the models in the estimation of the core damage frequency.

As noted, the first element of a Level 1 PRA identifies those sequences of events that, if not prevented, could result in a core damage state and the potential release of radionuclides. This process is typically divided into two tasks: identification of the initiating events and development of the potential core damage accident sequences associated with the initiating events.

The initiating event task involves identifying those events that challenge normal plant operation and that require successful mitigation in order to prevent core damage. There can be tens to hundreds of events that can challenge the plant. Individual events may, however, be grouped into initiating event classes, with classes defined by similarity of systems and overall plant response.

In the accident sequence development task, the different possible sequences of events that can evolve as a result of each initiator group are identified. The resulting sequences depict the different possible combinations of functional and/or system successes and failures and operator actions which lead to either successful mitigation of the initiating event or to the onset of core damage. Determination of what constitutes success (i.e., success criteria) to avert the onset of core damage is a crucial part of the accident sequence analysis task.

The second element of a Level 1 PRA involves the development of the models for the mitigating systems or actions in the core damage accident sequences. This task, referred to as systems analysis, involves modeling the failure modes of the plant systems which are necessary to prevent core damage as defined by the core damage accident sequences. This modeling process, which is usually done with fault trees, defines the combinations of equipment failures,

2 Level 1 PRA Modeling for Fullpower Operations

equipment outages (such as for test or maintenance), and human errors that cause failure of the systems to perform the desired functions.

The third element of a Level 1 PRA involves estimating the plant's CDF and the associated uncertainty. This process is typically divided into three tasks: data analysis, human reliability analysis, and quantification and uncertainty analysis.

The data analysis task involves determining initiating event frequencies, equipment failure probabilities, and equipment maintenance unavailabilities. Plant maintenance and other operating records are evaluated to derive plant-specific equipment failure rates and the frequencies of the initiating events. Where insufficient plant experience exists, failure rates and initiating event frequencies based on industry-wide "generic" data bases are used to complete the data base used in the risk analysis.

The human reliability analysis task is a key task in Level 1 PRA, involving modeling and evaluating the human actions important in the prevention of core damage. This evaluation both identifies the operator actions and quantifies the error probabilities of the identified actions. Human reliability analysis is a special area of analysis requiring unique skills to determine the types and likelihoods of human errors germane to the sequences of events that could result in core damage.

The quantification task integrates the initiating event frequencies, event probabilities, and human error probabilities to calculate the frequency of core damage and its associated uncertainty. As typically used in PRAs, the core damage frequency represents the average annual core damage frequency.

2.1.1 Accident Sequence Initiating Event Analysis

Initiating events are broadly categorized into two categories, internal initiating events and external initiating events. Internal initiating events are system and equipment malfunctions inside the plant. Analyzed along with internal initiating events is the loss of offsite electrical power. External initiating events include earthquakes, external flooding (i.e., from water sources outside the plant), transportation occurrences, and high winds. Note that many of these external events can cause a loss of offsite power in addition to other adverse impacts on the plant. Although internal flooding and fire events are conventionally treated in PRA studies as external events, they are included in the internal event category in this document. This section only addresses conventional internal initiating events that occur during full power operation including the loss of offsite electrical power. The special case of internal flooding and fires are addressed in Sections 2.2 and 2.3, respectively. Initiators during low power and shutdown operation and for external events are provided in Chapter 6.

2.1.1.1 Considerations for the Baseline PRA

This section defines the scope of initiating events that should be initially considered in a state-of-the-art PRA, as well as criteria for screening out initiators and grouping of the remaining initiators.

Initial Scope of Examined Initiators

In a full power PRA, internal events that cause an upset of normal plant operation that requires a reactor trip or unplanned controlled shutdown with the need for core heat removal are considered as initiating events. These events fall into one of two categories as follows:

- Loss-of-coolant accidents — All events that disrupt the plant by causing a breach in the primary coolant system with a resulting loss of core coolant inventory are modeled. These events include such occurrences as primary system pipe breaks, pressurized water reactor (PWR) steam generator tube ruptures (SGTRs), boiling water reactor (BWR) feedwater pipe breaks, interfacing system loss-of-coolant accidents (ISLOCAs), reactor pressure vessel (RPV) rupture, and BWR steam pipe breaks.
- Transients — All events that disrupt the plant but leave both the core coolant and other water systems' inventory intact are modeled. These occurrences include such items as automatic reactor shutdowns (scrams or trips), unplanned controlled reactor shutdowns (including those caused by degraded equipment configurations) manual reactor trips or scrams, manual operator actions taken in anticipation of degrading plant conditions, and transient-induced LOCAs. In identifying the transient events, frequently occurring events (such as turbine trips) and more rare events (such as loss of a support system) are considered.

When ensuring completeness in the initial list of initiating events (considered at the onset of the baseline PRA study), the analyst should have performed a comprehensive engineering evaluation that includes the following events:

- All general categories of events analyzed in Chapter 15 of the Final or Updated Safety Analysis Report (SAR) (e.g., increase or decreases in reactor coolant flow). The Chapter 15 analysis includes both transients and loss-of-coolant accidents (LOCAs).
- Events resulting in a loss of primary core coolant. This includes leaks and ruptures of various sizes and at different locations in the primary system (e.g., primary system pipe breaks, penetration failures, SGTRs and vessel rupture). In addition, a systematic search of the reactor-coolant pressure boundary should be performed to identify any active component in systems interfacing with the primary system that could fail or be operated in such a manner as to result in an uncontrolled loss of primary coolant (commonly referred to as ISLOCAs).
- All actual initiating events which have occurred at the plant. Actual plant scrams and unplanned shutdowns as documented in Licensee Event Reports (LERs) and scram reports should be included. These initiators typically involve faults in the nuclear steam supply system (NSSS) and in the turbine-generator and related systems (referred to hereafter as the balance-of-plant). Plant modifications (not accounted for in the baseline PRA) influencing occurrence rates should be considered.
- All initiating events considered in published PRAs (and related studies) of similar plants. NUREG/CR-4550 (Ref. 2.1) contains a list of transient initiating events that have actually led to reactor trips and that should be considered.
- All initiating events that have occurred at conditions other than full power operation (i.e. during low power or shutdown conditions) are included unless it is determined that they are not applicable to full power operation.
- All systems supporting the operation of other plant systems are reviewed to determine if their loss results in automatic scram, manual scram, or a controlled shutdown. Failure Modes and Effects Analysis (FMEA) are generally used to determine if an initiating event results from complete or partial failure of the system to operate, or from inadvertent operation of a system. In this method, the analyst determines for *each* component in the system: (1) its function, (2) the possible failure modes, (3) the failure mechanisms, and (4) the effects of the failure on the system and the plant.

2 Level 1 PRA Modeling for Fullpower Operations

A system is evaluated if its loss would disrupt the normal operation of the plant. At a minimum, support systems that are examined include alternating current (AC) and direct current (DC) buses, cooling water or service water systems, instrument and service air, heating, ventilation, and air conditioning (HVAC) systems throughout the plant (including the control room); and instrumentation/control systems.

In determining whether the loss of a plant system or component should be treated as a support system initiating event, the expected level of degradation to other plant systems (specifically, accident mitigating systems) is also determined and evaluated. This may require calculations to determine the resulting environment to which the mitigating equipment is exposed and comparison to equipment qualification information.

- Initiating events consisting of multiple equipment failures are included, if the equipment failures result from a common cause. For example, the failure of two DC electrical buses is included as an initiating event, if the failure is due to a common cause.
- For multiple unit sites where systems are shared or can be cross-tied, initiating events that can impact both units should be identified in addition to those that will only impact a single unit.
- An ISLOCA can be an important accident sequence because of its potentially significant contribution to the releases of radioactivity from the plant due to all possible accident scenarios. Therefore, the modeling of ISLOCAs and particularly the credit given for isolation of the ISLOCA, the predicted size of the ISLOCA, and the effects of the ISLOCA on other equipment can significantly affect the importance of this type of event.

NUREG/CR-5928 (Ref. 2.2) describes an acceptable approach to analyzing ISLOCAs at individual plants. In that report, a spectrum of topics are addressed including the modeling of ISLOCA sequences, the systems and components and their failure modes that should be considered, rupture probabilities for different types of components including different piping materials and designs, human reliability considerations for isolating or otherwise mitigating the LOCA, specific data suggestions for the analysis, and equipment effects considerations. Two additional specific considerations which may be in conflict with NUREG/CR-5928 for a specific plant and hence should be considered when analyzing ISLOCAs include the following:

- (1) Credit for motor operated valve (MOV) or check valve closure to isolate any resulting leak or rupture can only be taken in the PRA if supporting analysis/testing is available which demonstrates adequate capability of the valve for the expected conditions. This condition can be met by virtue of successfully addressing Generic Letter (GL) 89-10 for the valve(s) in question or by other supporting analyses or test results for valves (e.g., check valves) not covered by the licensee's 89-10 program (Ref. 2.3). With such supporting analyses, the nominal failure probability for valve closure can be used; otherwise it should be assumed that the valve will not close to isolate the breach.
- (2) Any resulting effects on equipment exposed to the breach should consider both the water and steam effects of the breach as well as propagation of that water/steam to other rooms or areas of the plant. Any credit taken for the continued operability of equipment in the expected environment should meet the attributes provided under the "equipment operability" issue discussed later. This includes consideration of whether the valve operators for MOVs will function to close the valve (even if the valve is determined capable of closing) given its exposure to the expected environment.

Screening Out Initiating Events

In a PRA, not every initiating event that causes a disruption of the plant has to be modeled. That is, accident sequences do not have to be developed for every initiating event. In some cases, it is allowable to exclude initiating events. Any of the following criteria can be used to exclude initiating events:

- The frequency of the initiating event is less than $1\text{E-}7$ /per reactor year (ry) when the initiator does not involve either an ISLOCA, containment bypass, or vessel rupture.
- The frequency of the initiating event is less than $1\text{E-}6$ /ry and the core damage could not occur unless at least two active trains of diverse mitigating systems are independently failed.
- The resulting reactor trip is not an "immediate" occurrence. That is, the event does not require the plant to go to shutdown conditions until sufficient time has expired during which the initiating event conditions can, with a high degree of certainty (based on supporting calculations), be detected and corrected before normal plant operation would be curtailed (either administratively or automatically).

For example, a steam generator tube rupture event may have a relatively low contribution to the total core damage frequency but may constitute a significant fraction of total large early releases. Initiating events such as these should not be excluded. The need to understand the potential consequences of an initiating event in order to exclude it from detailed analysis makes the process of excluding initiating events necessarily iterative.

As another illustration, the loss of switchgear room HVAC may not require the operator to initiate a manual shutdown for 8 hours based on a room heatup calculation. During this time, the operator can almost certainly detect and recover the fault using portable cooling equipment (as directed by procedures) and prevent the need for a forced shutdown. In this case, loss of switchgear room cooling could justifiably be eliminated as an initiating event (based on procedural guidance and calculational support).

The basis for excluding initiating events from detailed evaluation should have been established and documented for a peer review and users of the baseline PRA.¹ The fact that an event has never occurred, by itself, is not a sufficient basis for eliminating an initiating event from evaluation.

Grouping of Initiating Events

Numerous events and occurrences can disrupt a plant and the response of the plant to many of the events can be virtually identical. In such cases, it is acceptable to group the initiating events using the following criteria:

- Initiating events resulting in the same accident progression (i.e., requiring the same systems and operator actions for mitigation) can be grouped together. The success criteria for each system required for mitigation (e.g., the required number of pump trains) is the same for all initiators grouped together. In addition, all grouped initiators should have the same impact on the operability and performance of each mitigating system.

¹ The user (or reviewer) of this baseline PRA and its documentation need to compare the above criteria with those used for grouping initiating events in the PRA. Deviations should be noted especially when they have the potential for limiting the use of the baseline PRA.

2 Level 1 PRA Modeling for Fullpower Operations

and the operator. Consideration can also be given to those accident progression attributes that could influence the subsequent Level 2 analysis (refers to Chapter 3).

- In conformance with the criteria above, LOCAs can be grouped according to the size and location of the primary system breach. However, primary breaches that bypass the containment should be treated separately.
- Initiating events can be grouped with other initiating events with slightly different accident progression and success criteria if it can be shown that such treatment bounds the real core damage frequency and consequences that would result from the initiator. To avoid a distorted assessment of risk and to obtain valid insights, grouping of initiators with significantly different success criteria should be avoided. The grouping of initiators necessitates that the success criteria for the grouped initiators be the most stringent success criteria of all the individual events in the group. Note that in a sound baseline PRA, low-frequency initiators are grouped with other relatively high-frequency initiators, rather than excluding them from further analysis.

2.1.1.2 Application Impact Considerations

It is possible that a particular change to a plant's current licensing basis (CLB) may influence this task. The proposed change may result in:

- New accident initiators.
- Higher risk contribution of (initially) screened out initiator(s), and
- Change in the frequency of modeled initiator(s).

For every risk-informed regulatory change, the potential for these three items should be examined. This examination should consider structure, systems, and components (SSCs) modeled in the PRA as well as those SSCs not modeled. SSCs not modeled in the PRA should be subject to a failure modes and effects analysis (FMEA) (or equivalent) to assess their impact on accident initiators scope and frequencies.

Note that a proposed CLB change may necessitate reconsideration of the initiating events grouping scheme used in the baseline PRA to bring sharper focus on a subgroup of initiators that may be sensitive to the change.

2.1.1.3 Interface with Other Tasks

Results of reviews of this task should be considered before the onset of reviewing the data analysis (Section 2.1.4) and the accident sequence analysis (Section 2.1.2) tasks. A special emphasis should be given to limitations in the baseline PRA (or its documentation) related to scope, screening, and grouping of initiators which can compromise the soundness of results of these two interfacing tasks, and consequently the adequacy of the baseline PRA to support the proposed risk-informed applications.

2.1.1.4 Documentation

The documentation of the initiating event task should be sufficient such that a peer reviewer can reproduce the results. At a minimum, the following information pertinent to initiating events should be documented:

- A list or general description of the information sources that were used in the task.

- Specific information/records of events (plant specific, industry experience, "generic" data) used to identify the applicable initiating events.
- The initiating events considered including both the events retained for further examination and those that were eliminated, along with the supporting rationale.
- Any quantitative or qualitative evaluations or assumptions that were made in identifying, screening or grouping of the initiating events as well as the bases for any assumptions and their impact on the final results.
- Documentation of the FMEA performed to identify support system initiators and the expected effects on the plant (especially on mitigating systems).
- Specific records of the grouping process including the success criteria for the final accident initiator groups.
- Documentation of findings of FMEA (or equivalent) performed on SSCs within the scope of the change but not modeled in the PRA, to assess their impact on the scope and frequency of initiators.

2.1.2 Accident Sequence Analysis

The objective of the accident sequence analysis task is to determine the possible plant responses (sequences) that could occur as a result of initiating events. These plant responses are defined in terms of the different possible combinations of successful and unsuccessful functions or systems and operator responses required to mitigate an accident initiator. For the Level 1 portion of an analysis, the following discussion is provided for those plant responses or sequences that end with either the plant in a stable state or when the plant has entered into a "severe accident" state in which the onset of core damage is imminent.

Accident sequences are determined by implementing a logical method for identifying the different possible plant responses to the initiating events. The plant safety functions and corresponding plant systems and operator responses that need to occur to mitigate each initiator are used to represent the different possible plant responses (or accident progressions sequences).

Different models can be used to develop the accident sequences. Among these, the two principal methods used are event sequence diagrams and event trees. There are also different types of event trees (e.g., functional versus systemic) and different ways of documenting the response to each accident initiator (e.g., separate event trees for each initiating event group or a general tree with the initiating event impacts included in system fault trees, or inclusion of support systems and shared equipment in the event tree rather than at a fault tree level). All of these different event tree approaches can be used. The following discussion presents the attributes of the event tree approach to accident sequence analysis since it is the most prevalent technique.

2.1.2.1 Considerations for the Baseline PRA

This section identifies several key factors to consider in evaluating the baseline PRA used in a risk-informed regulatory application.

2 Level 1 PRA Modeling for Fullpower Operations

Establishing Success Criteria

Accident sequence analysis establishes the success criteria which should be met to prevent core damage. The success criteria are thus dependent on the definition of core damage. Core damage has been defined in the past PRAs in various ways, usually through peak cladding temperature limits or designated levels in the vessel. The onset of core damage generally means that no imminent recovery of sufficient coolant injection is anticipated, and therefore, a substantial amount (equivalent to or greater than the design basis) of the radioactive material contained in the gap between the cladding and the fuel is subsequently released. Comparable definitions that result in essentially the same phenomena can be used. Whatever the definition chosen for the onset of core damage, it should be supported by calculations. Note that considerable fuel melting may also be expected in most accident sequences with core damage outcomes.

The accident sequence model may include as the event tree headings the necessary safety functions, systems, and operator responses to prevent the onset of core damage. Accident sequence models can also delineate the functions required to protect the containment and influence the amount of radioactive material released.² The safety functions modeled in a Level 1 PRA include reactivity control, reactor coolant system (RCS) overpressure protection, reactor coolant inventory control and heat removal, and containment over-pressure protection (both early and late). The containment over-pressure protection functions are listed in the Level 1 considerations because the containment condition can adversely impact the core heat removal and inventory control functions.

The success criteria for each of these functions required to prevent core damage should be established (e.g., the RCS inventory control function can be expressed in terms of required flow rate). Once established, the system and operator responses modeled in a PRA include those frontline, support systems, and operator actions needed to successfully meet the modeled safety function success criteria. The minimum hardware for each identified system (e.g., the number of pump trains) and operator responses required to meet the function success criteria determine the success criteria for responding to each initiating event group.

The use of realistic success criteria provides additional assurance that the relative importance of the quantified accident sequences is as accurate as possible. To further ensure a "realistic" analysis, the use of success criteria which are excessively limiting (such as the success criteria used in design basis assessments) is avoided. For example, the licensing basis may require two out of four emergency core cooling pumps when "best estimate" calculations show that only one out of four pumps will prevent the onset of core damage.

"Realistic" success criteria, rather than the licensing-bases criteria, can be used for both the safety functions and the individual systems that perform those functions. Therefore, the evaluation does not have to stop with safety-related systems when non-safety related equipment may be available to perform the needed function, thereby, preventing the onset of core damage.

For grouped initiators, the accident sequence modeling should reflect the most stringent initiator. For example, the coolant injection requirements for LOCA initiators (which usually involve a spectrum of break sizes) are based upon

²The attributes provided in this section do not address event trees where the end state goes past the onset of core damage. Functions required for establishing the containment performance and release of radioactive material are identified in the Level 2 discussion. Further event tree modeling to establish plant damage states is not addressed in this section.

the upper end of the break spectrum. For other functions, the requirements may have to be based upon a different initiator included in the group.

The success criteria for preventing core damage can be dependent on the accident progression and timing. For example, for a BWR, the control rod drive (CRD) system may not provide sufficient flow for coolant injection at the beginning of a small LOCA; however, at 4 hours into the accident (given coolant injection has been occurring), the coolant inventory requirements are reduced and CRD flow is adequate. In addition, the time required to align a system may influence what time frame it can be credited in (e.g., firewater may not be credited early on in an accident (e.g., a LOCA) since it could require connection of multiple fire hoses, insertion of spool pieces, or opening of remote valves.

In determining "realistic" success criteria, particularly when such criteria are considerably different from the SAR design basis or is not even addressed in the SAR, supporting analyses (e.g., thermal-hydraulic calculations) should be the basis for the success criteria that is credited in the PRA. Representative examples of criteria often used in PRAs that differ considerably or are not addressed by the design basis criteria are (a) feed and bleed mode for PWR core cooling, (b) primary/secondary system depressurization and use of low pressure safety injection and/or condensate to the steam generators whenever high pressure safety injection and/or main and auxiliary feedwater are unavailable in PWRs, and (c) in case of BWRs, use of alternate injection systems (such as control rod drive flow or firewater) under conditions when all other injection systems are unavailable. These represent conditions that go well beyond the single failure considerations applied in the design basis and hence did not have to be treated in the original licensing basis for the plant. While plant-specific calculations are preferred, non-plant specific calculations (e.g., use of "similar" plant analyses perhaps with modification) are acceptable provided appropriate justification is established. The computer codes used to calculate success criteria (either plant-specific or for a similar plant) should contain the modeling detail present in codes such as RELAP and TRAC (Ref. 2.4) and should be verified for the conditions that exist in the success criteria application.

For instance, anticipated transient without scram (ATWS) represents a complicated and "beyond design basis" set of scenarios requiring analysis and supporting calculations to properly characterize the success criteria. The estimated risk contribution of ATWS events is in part a function of modeling approaches and associated assumptions used in interpreting the success criteria. For PWRs, what constitutes successful pressure control often sets the stage for the rest of the analysis. An acceptable basis for successful pressure control is the use of the stress Level C limits of the American Society of Mechanical Engineers (ASME) code for the assumed failure point for the vessel and primary piping from overpressurization. Supporting calculations (preferably plant-specific) are performed to address the critical Moderator Temperature Coefficient (MTC) necessary to ensure the unacceptable stress limit is not reached (i.e., the portion of the fuel life when the MTC is sufficiently negative). Furthermore, plant-specific analyses are preferred to determine the pressure increases associated with failure to trip the turbine during an ATWS. For BWRs, a similar basis for success during an ATWS can be established and then plant-specific considerations are used to interpret the need for:

- Recirculation pump trip (RPT) including whether all pumps should trip.
- Standby liquid control (SLC) system operation particularly the time the system should be initiated for successful mitigation.
- Inhibiting emergency core cooling system (ECCS) injection inside the shroud and inhibiting automatic depressurization.

2 Level 1 PRA Modeling for Fullpower Operations

- Requirement for vessel level control during injection by both high and low pressure systems.
- Containment and suppression pool cooling to avoid adverse impacts on continued operability of core cooling.

One concern regarding accident sequence modeling is the loss of reactor coolant pump (RCP) seal cooling. Such a concern arises during consideration of loss of pump cooling events and loss of all AC events, both of which cause a loss of pump seal cooling and the potential for a primary system LOCA (through the pump seals) requiring reactor coolant makeup. Pump seal failures can also be initiating events for the PRA.

The proper model depends on the pump manufacturer (Westinghouse, Byron Jackson, Bingham) and the seal design. Another consideration which may make a difference is whether or not the pump has been tripped upon loss of seal cooling/injection. In addition, there is a range of opinion as to what would be the proper seal leakage model (meaning the probability of a certain flow rate vs. time) for a given pump. The chosen model can significantly affect the results by considerably altering both the ranking of dominant accident sequences as well as affecting the overall core damage frequency. The treatment of RCP seal LOCAs is an example of an area where there is a considerable variation and uncertainty in the accident sequence modeling.

Because of the less than definitive conclusions that have been made as to the appropriate model to use for PRA purposes, this document provides suggested RCP seal LOCA models for incorporation into PRAs and PRA applications until (and if) more information becomes available. Alternate models may be used provided justification is provided for their use. The suggested model approaches provided below are based on the conclusions of the related elicitation issue in the NUREG-1150 study (Ref. 2.5), and consider the modeling approaches used by the licensees in their individual plant examinations (IPEs).

Case 1 - Pumps-tripped condition:

The RCP seal leakage model is based on the discussion in Section 5 of NUREG/CR-4550 (Ref. 2.6). A licensee may wish to group similar leak rates from the tables in Section 5, but needs to consider the full range of possible leak rates and probabilities provided in the referenced report. It is suggested that an acceptable approach for plants with the Westinghouse "old" o-ring design pumps is to use the "old" o-ring values (or a suitable equivalent, with justification provided). It is also suggested that an acceptable approach for plants with the newer, more temperature tolerant Westinghouse design (and all other pump manufacturer designs) is to use the "new" o-ring design values (or a suitable equivalent, with justification provided).

Case 2 - Pumps-not-tripped condition:

The licensee determines the maximum possible flowrate for the applicable pump manufacturer assuming the seals (all stages) are destroyed and no longer provide a flow restriction within the labyrinth. The calculated flowrate is assumed to occur by 30 minutes following the initiating event.

The significance of the above models to the PRA results is still dependent on such factors as the number of pumps affected, cooling system configuration, and hence probability associated with a total loss of pump cooling, the ability to provide reactor coolant system injection during such conditions (for instance, the BWRs, except for some of the older designs, are generally better able to cope with such a LOCA even under loss of all AC power because of their high-pressure coolant injection (HPCI) and reactor core isolation cooling (RCIC) systems), etc.

Modeling Accident Progressions

The modeling of the accident sequence progressions necessitates that the response of the plant systems and the operator accurately reflect the system capabilities and interactions, procedural guidance, and the timing of the accident sequences. Therefore, the development of the accident sequence models should correctly incorporate the planned response to an initiator that exists in the plant emergency and abnormal operating procedures and as practiced in simulator exercises. In fact, the procedural guidance along with timing information obtained through thermal-hydraulic calculations serves as the guide in the actual development of the accident sequence models. Operator actions required to mitigate an accident sequence (e.g., manual initiation of systems or special actions such as controlling vessel level during an ATWS in a BWR) should be modeled (see Section 2.1.5). Therefore, event tree headings should be chronologically placed in the order that the system or operator action is expected to be challenged. Deviations from the chronological representation of the procedural guidance should be well documented.

In developing the accident sequences, the accident progression (as represented by the logic structure of the model) should also account for dependencies and interfaces between and among the plant safety functions, systems and operator actions needed for accident mitigation. The dependencies and interfaces that should be considered include functional, phenomenological, and operational dependencies and interfaces.

Functional dependencies exist where the success of one function is dependent or otherwise affected by the success/failure of another function. There are two dependencies that should be addressed. These dependencies include (1) interaction of the initiating group with mitigating systems and operator actions, and (2) interaction among the mitigating systems and operator actions.

The interactions of the initiating event group with available mitigating systems and actions are accounted for either in the accident sequence model or at the system model level. Both immediate effects (e.g., loss of systems such as the power conversion system (PCS) following loss-of-offsite power) and delayed effects (e.g., loss of a system due to a loss of HVAC should be included. Delayed impacts can be subtle and require that both harsh environmental impacts (discussed in more detail below) and protective trip logic be considered. An example of protective trip logic concerns is the occurrence of a steam leak detection trip signal resulting due to a high room temperature that could result from a loss of room cooling. The loss of room cooling may occur for various initiators including loss of offsite power, loss of a cooling water systems, or loss of the HVAC system itself.

The interactions among mitigating systems and operator actions are also accounted for either in the accident sequence model or at the system model level. One type of interaction is the successful operation of a system precluding the need for a redundant system performing the same function. The second type of interaction is the failure of one system precluding the operation of another system. An example of these types of functional dependencies in both a BWR and PWR is the requirement for the success of primary system depressurization before low-pressure coolant injection can be utilized. Alternatively, vessel depressurization may cause loss of a system due to pump run-out inducing a subsequent pump trip. Another common example of a functional dependency is that battery depletion during a station blackout precludes continued operation of steam-driven systems.

Phenomenological dependencies manifest themselves where the environmental conditions generated during an accident sequence influence the operability of systems and equipment. Phenomenological impacts can include generation of harsh environments that result in protective trips of systems (e.g., due to high pressures or temperatures), loss of ECCS pump net positive suction head (NPSH) when containment heat removal is lost, clogging of pump strainers from debris generated during a LOCA, failure of components outside the containment following containment failure due to the

2 Level 1 PRA Modeling for Fullpower Operations

resulting harsh environment, closure of safety relief valves (SRVs) in BWRs on high containment pressure, and coolant pipe breaks following containment failure.

Phenomenological impacts can also be indirect. For example, failure of containment heat removal in a BWR should cause the operator to depressurize the vessel per procedures to maintain suppression pool heat capacity limits. Such an action can result in loss of driving steam for systems such as HPCI and RCIC. Circumvention of some of these failure modes such as bypassing of protective trips, switching suction sources for pumps, and arranging alternate room cooling can be credited either in the accident sequence modeling or system models if the action can be realistically accomplished considering available staffing, the available time to perform the action, and any harsh environment where the actions should be performed. Most of these phenomenological dependencies are identified on an individual system basis as part of the systems analysis (see Section 2.1.3).

Operational dependencies that are hardwired or are configuration dependent are present for some systems or components. An example of an operational dependency is that the suppression pool cooling mode of a loop of residual heat removal is not available when the system is in the low pressure coolant injection mode.

Consideration should also be given to sequences in which the nature of the accident changes. For example, an initial transient may become a LOCA event due to reactor coolant pump seal failure or a demanded and stuck open primary relief valve. Proper modeling of this progression change accounts for any dependencies among events previously discussed. Transfers to other sequence models to reflect the change in the sequence should be made with due consideration given to any differences between the modeled initiators. Screening of such transfers can be performed but should follow the truncation considerations provided in Section 2.1.6 (sequence quantification) and should be reevaluated for each risk-informed regulatory application.

2.1.2.2 Application Impact Considerations

It is possible that a particular change to a plant's current licensing basis (CLB) may affect the accident sequence analysis task. The proposed change may result in:

- New/fewer event trees being considered;
- Revised success criteria;
- New dependencies or interfaces;
- New/fewer and/or rearranged event tree headings due to changes in procedures, equipment, technical specifications, etc.;
- Revised sequence logic.

2.1.2.3 Interfaces with Other Tasks

Initiating event analysis and systems analysis will provide information on the impact of initiating events on mitigative functions. Systems analysis and human reliability analysis (HRA) will provide information on the interactions among mitigating systems and operator actions, phenomenological interactions and operational dependencies. Systems analysis will provide information used to obtain success criteria and accident progression. Thermal-hydraulic analysis

is used in various aspects of this task, e.g., for success criteria, timing, environmental effects, etc. The output of the sequence analysis is used as an input the HRA task, and to generate cutsets used for sequence quantification task. The sequence analysis will also guide the systems analysis, as reference is made to certain systems or functions in the event trees and the success criteria.

2.1.2.4 Documentation

The following information concerning the accident sequence modeling should be reported:

- A list or general description of the information sources that were used in the task.
- The success criteria established for each initiating group including the bases for the criteria (i.e., the system capacities required to mitigate the accident and the necessary components required to achieve these capacities).
- The event trees or other types of models used (including all sequences) for each initiating event group.
- A description of the accident progression for each sequence or group of similar sequences (i.e., descriptions of the sequence timing, applicable procedural guidance, expected environmental or phenomenological impacts, dependencies between systems, and other pertinent information required to fully establish the sequence of events).
- Any assumptions that were made in developing the accident sequences, as well as the bases for the assumptions and their impact on the final results.
- Existing analyses or plant-specific calculations performed to arrive at success criteria and expected sequence phenomena including necessary timing considerations.
- Sufficient system operation information (refer to the following section) to support the modeled dependencies.
- Input, calculations, etc. (particularly to justify equipment operability beyond its "normal" design parameters and for which credit has been taken).
- How the application changes the baseline model in this task.

2.1.3 Systems Analysis

There are different analytical techniques that can be used to perform or support a systems analysis. Examples include: FMEA, reliability block diagrams, and fault trees. Fault trees are the preferred method since they are deductive in nature and, if properly performed, can identify all potential failure modes of a system and thus can be used to calculate the unavailability of the system.

2.1.3.1 Considerations for the Baseline PRA

Detailed fault tree models are generally required in analyzing the system, although sometimes, a simplified fault tree or the black box approach (treating the system as a basic event) is acceptable, as delineated below. The basic concepts

2 Level 1 PRA Modeling for Fullpower Operations

for constructing fault trees are described in "The Fault Tree Handbook" (Ref. 2.7). Some considerations applicable to this method are discussed below.

A fault tree can be simplified to include only the dominant types of failures. A single data value, for systems where sufficient experience exists, can be used to represent system's unavailability. In such cases, care should be taken to model those aspects of the system which form dependencies with other systems so that dependent or common cause events are properly handled.

An example of where a simplified fault tree could be utilized is for the automatic depressurization system (ADS) system in a BWR. Here, common cause valve failure and an operator error to manually initiate the system have been shown to be the dominant failure modes for the ADS. Since this system is dependent on several support systems (DC power and instrument air) used by other systems, these support system interfaces would have to be modeled. An example of where a data value is permissible is the reactor protection system (i.e., the failure to scram the reactor). In this case, the reactor protection system (RPS) failure modes are independent of other system failures.

Establishing System Analysis Boundaries

An accurate representation of the design, operation and maintenance of each modeled system is essential. The design, operation and maintenance requirements and practices are reviewed to ensure that the system model reflects the as-built and as-operated system. System walkdowns are performed to confirm the design of the system. Operator interviews, system procedure (abnormal, operating, maintenance, and testing) reviews, and involvement of plant system engineers are also necessary.

The failure criteria defining the top event of the fault tree for each system should match the accident sequence success criteria. Note that in some cases, multiple models for the same system may be needed to address different sequences.

All equipment and components necessary for the system to perform its function (as defined by the accident sequence success criteria) during the postulated accident mission time are considered in the system model. The boundaries of these equipment and components should also be defined. These definitions should match a level of detail where statistical data exists in determining their failure probabilities. In addition, the defined boundaries should be able to reflect the dependencies and interfaces between equipment and systems.

All relevant and possible failure modes for each component should be considered. These failure modes generally include the following:

- Hardware faults
 - Failure to change state
 - Failure to operate
- Out-of-service unavailability
- Common cause faults
- Operator faults
- Conditional operability faults including equipment capability and phenomenological faults

Hardware faults are those physical breakdowns of the equipment such that the system or component cannot function as designed (e.g., pump shaft breaks).

In modeling the out-of-service unavailability, both planned and unplanned test and maintenance contributions are considered. The type of testing and maintenance modeled should be consistent with the actual practices of the plant for removing equipment from service for maintenance. These considerations might include technical specification equipment configuration control violations as well as previously identified implementation and program deficiencies with the equipment configuration control process.

Common cause equipment failures are multiple failures that result from a single event or failure. The NRC's Office of Analysis and Evaluation of Operational Data (AEOD) report, "Common Cause Failure Data Collection and Analysis System" (Ref. 2.8) presented in six volumes, provides a suggested common cause failure modeling approach. Volumes 5 and 6 of that report are particularly useful as they directly apply to the modeling (Volume 5) and the database (Volume 6) applicable to PRA. Given the current state-of-the-art of common cause failure analysis and the data available, only intra-system common cause failures are generally modeled. Inter system common cause failures should be considered when indicated, as is commonly done in the case of the BWR HPCI-RCIC systems, cited in the AEOD report.

How common cause events are included in the model may vary (e.g., included in the system fault trees, added after initial cutset review of independent failure combinations) but the approach should demonstrate that quantitatively important common cause combinations are not missed. Truncation considerations should be consistent with those expectations provided in section 2.1.6, accident sequence quantification (i.e., truncation of any common cause events would be based on low cutset frequency arguments). In addition, the truncation of any common cause events should be reevaluated for every risk-informed regulatory application of the PRA. For cases where the PRA involves the evaluation of common cause among a component type not covered by the AEOD report, the component type closest in design and similarity in the AEOD report can be used to perform the evaluation. In evaluating the human error probabilities, the analyst would also consider common causes and incorporate performance shaping factors (PSFs) to account for dependencies.

Certain types of human error events should also be considered in the systems analysis. These events include, at a minimum, those human actions that cause the system or component to be inoperable when demanded. These events (also referred to as pre-initiator human events) are analyzed as part of the human reliability analysis, discussed in Section 2.1.5. Other human events can be included in the systems analysis model. These events include those actions needed for the operation of the system or component. These events (also referred to as post-initiator human events) are also analyzed as part of the human reliability analysis, discussed in Section 2.1.5.

System models should also treat conditional faults. These failures are discussed below under system dependencies and interfaces.

Supercomponents or modules can be used. However, the modularization process should be performed in a manner that avoids grouping events (i.e., component failures, testing and maintenance unavailabilities, and human errors) with different recovery potential (e.g., hardware failures that cannot be recovered versus actuation signals which can), human error events, events which are mutually exclusive of other events not in the module, and events which occur in other fault trees (especially common cause events). Note that some risk-informed regulatory applications of PRA may necessitate certain events to be removed from modules.

2 Level 1 PRA Modeling for Fullpower Operations

Modeling System Dependencies and Interfaces

A PRA should model the dependencies and interfaces between and among the systems and components. At a minimum, the following dependencies and interfaces should be modeled:

- **System Initiation, Actuation and Operation** — those systems that are required for initiation, actuation and continued operation of the system (i.e., for both the frontline mitigating systems and support systems) are identified, e.g., AC and DC power and instrument air. In modeling the initiation and actuation of a system, conditions needed for initiation and actuation (e.g., low RPV water level) should also be addressed. For example, a condition required to initiate a system automatically may not exist in some accident sequences. Thus, failure of that portion of the automatic actuation system has a probability of 1.0 for those accident sequences.
- **System Isolation, Trip or Failure** — those conditions that can cause the system to isolate or trip and those conditions that once exceeded can cause the system to fail. At a minimum, conditions that are considered include environmental conditions, fluid temperature and pressure being processed, external water level status, water and air temperature, pressure, humidity, and radiation levels. These conditions may arise when other systems fail to function. Examples of required systems include HVAC, service/component cooling water, heat tracing on piping and tanks to prevent boron solution precipitation, instrumentation (pressure, temperature, level, etc.), and water transfer systems to maintain tank levels.

Examples of conditions that can isolate, trip or fail a system or component include:

- For BWRs, high pressure in the RPV will prevent opening of the low pressure injection system isolation valves.
- A diesel generator will trip when the high jacket water temperature setpoint is reached. This condition can occur when the supporting cooling water supply to the diesel generator is lost.
- Inadequate pump NPSH due to low suction source level or high temperatures, clogging of strainers, steam binding of auxiliary feedwater pumps, and steam environment effects are a few example of conditions that can fail pumps.

Because of the attempted realistic nature of PRAs, there are many examples of where allowance is made for the operability of equipment beyond its design basis. This credit is allowed to account for the design margins built-in to most equipment used in a nuclear power plant and hence to recognize that equipment may function in conditions that are beyond those accounted for in the design basis. Examples include operability of pumps under saturated water suction conditions, steam relief valve operability even when the valve is operating under two-phase flow conditions, battery operability given all charging to the batteries has been lost, human performance under undesirable environment or radiation conditions, etc.

While crediting the potential for this operability supports the intent to provide a realistic analysis, such judgments of operability can often "drive" the results of the analysis and significantly impact the dominant sequences and contributing equipment that most affect the core damage frequency estimated in the PRA; therefore, such judgments should be supported. Test data, actual plant experience, vendor information regarding experience of similar equipment in other applications, and technical analyses are examples of

acceptable evidence. Otherwise, it should be assumed that once the expected conditions in the scenario exceed the design basis limits for the equipment, the equipment then fails with a probability of 1.0.

- **System Capability** — those conditions that can cause the system, though operable, to not meet the required function. Examples of this nature include flow diversion and insufficient inventories of air, water or power to support continued operation of the system for the assumed mission time. Such "failures" are explicitly treated in the modeling process using realistic operability considerations and should be supported with analysis; otherwise, it should be assumed once these conditions exist that the equipment/system fails with a probability of 1.0.
- **Shared equipment** — those components and equipment that are shared among systems. Passive components not typically modeled are included when their failure impacts more than one system (e.g., a discharge pipe from a tank feeding two separate systems).

Screening and Excluding Components and Failure Modes

It is not always necessary to model every component or failure mode. However, certain risk-informed regulatory applications of the PRA may necessitate that components and/or failure modes not generally included be added to the system models.

In screening or excluding components or failure modes, the following criteria are suggested:

- **Screen/Exclude Component** — The *total* failure probability of the component (sum of all failure modes) is at least two orders of magnitude lower than the next highest failure probability of another component in the same system train *and* the component (to be screened/excluded) does not have any dependencies or interfaces with other components or systems. In some cases passive components are excluded based on the fact that failure rates for these components are substantially less than active components.
- **Screen/Exclude Failure Mode** — The probability of the failure mode is at least two orders of magnitude lower than the next highest failure probability of another failure mode of that component (and there is no high potential for common cause failure). An example is the probability of spurious closure of an MOV compared to the probability of it failing to open.

2.1.3.2 Application Impact Considerations

It is possible that a particular change to a plant's CLB may affect the systems analysis task. The proposed change may result in:

- Additional/fewer systems being modeled.
- A change in modeling of component/system unavailability.
- Additional/fewer components may be modeled.
- The type of component failure modes included in the model.
- Change in common cause modeling.
- Change in HRA modeling within the system's fault tree.
- Component/system operability limits may change.
- Removal of events from the supercomponent modules, or addition of events to them.

2 Level 1 PRA Modeling for Fullpower Operations

2.1.3.3 Interfaces with Other Tasks

The sequence analysis task identifies the plant systems that need to be analyzed. Data analysis task interfaces with the systems analysis task to insure that the same events are treated in both and that the component boundaries are the same in both. Systems analysis task may provide some initiating events and assesses the impact of initiating events on systems (used in sequence analysis). Systems analysis cutsets may be used to generate sequence cutsets. It also provides information on various types of dependencies for the sequence analysis. Information on success criteria and accident progression is also provided.

2.1.3.4 Documentation

The following system analysis information should be documented:

- A list or general description of the information that was used in the development of the system models, including a brief discussion of the following:
 - System function and operation under normal and emergency operations
 - Actual operational history indicating any past problems in the system operation
 - System success criteria and relationship to accident sequence models
 - Human actions necessary for operation of system
 - List of all test and maintenance procedures
 - System schematic illustrating all equipment and components necessary for system operation
 - Records/notes of walkdowns and significant discussions with plant staff
 - System dependencies and shared component interfaces documented using a dependency matrix or dependency diagram indicating all dependencies for all components among all systems (frontline and support)
 - Table listing failure modes modeled for each component and event quantification
 - General spatial information and layout drawings to support external event analyses
 - Assumptions or simplifications made in development of specific system models.
- The nomenclature for the basic events modeled.
- The freeze date used to represent the design and operation of the plant.
- Any general assumptions that were made in the development of the systems models, as well as the bases for the assumptions and their impact on the final results.
- List of all components and failure modes included in the model, along with justification for any exclusion of components and failure modes.
- Information and calculations to support equipment operability considerations and assumptions.
- References to specific controlled input documents used for modeling (e.g., piping and instrumentation diagrams).
- Documentation of modularization process (if used).

- Records of resolution of logic loops developed during fault tree linking (if used).
- How the application changes the baseline model.

2.1.4 Data Analysis

The input parameters for the Level 1 portion of the PRA includes initiating event frequencies, equipment reliabilities, unavailabilities due to out-of-service time, and common cause failure probabilities and associated uncertainty distributions. For each of these four types of parameters, the task activities includes: identifying the data sources, selecting and screening the raw data, and quantifying data parameters.

2.1.4.1 Considerations for the Baseline PRA

The following points are typically considered in performing data analysis:

Initiating Event Frequencies

Selection and grouping of initiating events following the discussion in Section 2.1.1 would form the basis for reviewing and identifying the particular plant events or generic data that could be used for estimating the initiating event frequencies. For transient initiating event frequencies, the number and nature of plant scrams and unplanned shutdowns and the hours the generator is on line should be identified. For initiators where there is little or no plant-specific events, generic initiating event frequencies should be used for establishing prior distributions for Bayesian updating with available plant specific data. NSAC-182 (Ref. 2.9) provides data on the frequency of loss-of-offsite power (LOOP) events. NUREG/CF-5032 (Ref. 2.10) provides an acceptable method of Bayesian updating with plant-specific data. Expert judgement elicitation can be performed according to the method in NUREG/CR-4550, for estimating special parameters such as constructing the site specific seismicity curve for seismic analysis. Certain initiator frequencies (e.g., loss of support systems) may be estimated by constructing and quantifying plant-specific fault trees.

Equipment Reliability

The relevant parameters for equipment reliability are the demand failure probability (for standby equipment, required to start or change state), and the operating failure rate (for equipment that should operate for some time after an accident or transient to mitigate its effect or impact.) The preferred method for estimating equipment reliability parameters is Bayesian updating in which generic data are used as a prior distribution and updated with plant-specific data. Generic data sources should be representative of the plant components and the nature of the failures and demands in the pooled data set should be consistent with the plant specific applications modeled in the PRA. Generic data used in the model would be pedigreed and justified for the applicability to the specific plant under study. The component boundaries and failure modes defined in the model are to be consistent with those in generic and plant-specific data. EPRI/TR-100381 (Ref. 2.11) provides useful information on the process for data collection, and reduction along with examples of equipment boundaries. The raw data needed to estimate these parameters are the number of demands, the number of demand failures, the number of failures observed while running and the running (operating) time.

In quantifying component reliability, actual demands and those that reasonably approximate conditions for the required accident/transient response should be used. For those cases where demands are not normally tracked (e.g., using a safety pump to regularly fill a tank), demands can be estimated based on establishing a representative history.

2 Level 1 PRA Modeling for Fullpower Operations

Demands and their associated failures should be collected and tabulated by the nature of the demand (i.e., actual, spurious, type of test, etc.). Pooling demands and associated failures can be done when 1) the nature of the demands are similar, 2) the nature of the failures are similar, and 3) the failure probabilities from the pooled sources represent similar statistical populations.

Data used in the component failure probability estimations should be representative of the current component design and operation. Therefore, failure events may be examined in detail to show if plant modifications have eliminated the types of failures previously identified and have not introduced other credible failure mechanisms not previously observed. Failures recovered promptly from the control room such that the function of the component was not compromised can be excluded as failures from the data set, provided that the model does not credit such recovery elsewhere. Repeated failures occurring within a small time interval should be counted as a single demand and a single failure if there is a single, repetitive problem that causes the failures. (For example, if a valve fails to open and subsequently receives multiple demands to open, only one failure and one demand should be counted.) For failures discovered by means other than a valid demand, the equipment unavailability resulting from such a failure should be counted against the accumulated equipment unavailability. (For example, an operator discovers while taking log readings that a pump has no oil in its lubrication reservoir rendering it inoperable.)

The failure to run rate is used for operating equipment that should operate for an extended period following a demand. This would normally be a time after which the equipment reached rated speed or voltage and ran long enough to be judged a successful start (generally an equilibrium operating state.) The data needed (for equipment normally in standby) are the cumulative hours of operation after a successful start and the number of failures observed during these hours of operation. For equipment normally operating, the data needed are the cumulative operating time and the number of failures observed during these hours of operation. For test surveillance or other demands for which the actual run times are distinctly less than the length of the mission time modeled in the PRA, it should be determined whether the failure rate derived from truncated tests or demands is applicable over the mission time.

The statistical estimation techniques would consider the types of parameters to be estimated, and availability of generic or plant-specific data in "raw" or "treated" forms. These considerations should also include the choice of prior distribution in case Bayesian techniques are implemented.

Equipment Unavailabilities

Out-of-service unavailability data are needed for equipment removed from service for planned or unplanned repair or testing. The data required are the out-of-service time for each component and the total time the component is required to be operable. Coincident outage times for redundant equipment (both intra- and inter-system) should be examined and accounted for based on actual plant experience. Calculations of outage unavailabilities should reflect actual plant experience.

Common Cause Failures

Options for estimating common cause failure (CCF) parameters are: (1) Alpha factor models, (2) the Beta factor model, (3) the Multiple Greek Letter model, and (4) the Binomial failure rate model. The data needed for estimating common cause failure probabilities are the number of independent failures and the number of multiple failures due to a common cause. Since there is generally insufficient data to derive plant-specific estimates of the common cause failure parameters, generic data should be used. However, the generic data should be evaluated to determine their applicability to a specific plant. In those cases where some plant-specific data are available, they can be used to update

the generic data with Bayesian methods. The methods and database from the AEOD report (Ref. 2.8) could be used for deriving common cause failure probabilities.

2.1.4.2 Application Impact Considerations

It is quite likely that proposed changes to the CLB impact the results of data analysis and the estimated parameters. The proposed changes may result in:

1. Changes in the frequency of modeled initiator(s).
2. Changes in the estimated component unavailability contribution due to out of service time.
3. Changes in the estimated component unavailability contribution due to changes in the component failure rates, and
4. Potential changes in CCF contributions and new CCF mechanisms.

For every risk-informed regulatory change, the potential for these four items should be examined. This examination should consider SSCs modeled in the PRA as well as SSCs not explicitly modeled (specially those capable of impacting the initiating event frequencies). Plant specific experience data, industry wide experience data, and the appropriate engineering and reliability model could be used for such examinations.

2.1.4.3 Interfaces with Other Tasks

Review findings and considerations for selecting, screening, and grouping initiating events (Section 2.1.1) would be used as needed in refining the initiating event frequencies. The mission times used for component reliability estimations are provided by the accident sequence analysis task. The component specification, failure mode identification, and its initial operating conditions are determined from system analysis task. System analysis task also identifies the group of components for CCF analysis and the potential CCF mechanisms. The results from data analysis are used for accident quantification task.

2.1.4.4 Documentation

The following information is normally in the baseline PRA documentation. This information would be revised or supplemented as needed following the completion of this task. This information includes:

- The initiating event frequencies.
- The distribution for demand failure probability, standby failure rate, failure-to-run failure rate, and equipment out-of-service unavailability (as applicable) for each event.
- System and component boundaries, mission times, and reliability models used.
- The sources of raw data, generic data, and other information used in estimating initiating event frequencies, equipment reliability, or CCF probabilities.
- The time period from which plant-specific data were gathered.

2 Level 1 PRA Modeling for Fullpower Operations

- Key assumptions made in the data analysis. (The bases for the assumptions and their impact on the final results should be discussed in the sensitivity analyses.)
- Raw data records and related interpretations of those records used to derive the data values should be available for review, but need not be part of the PRA submittal.
- Rationale for and distributions used as priors for Bayesian updates.
- Changes resulting from the proposed CLB changes.

2.1.5 Human Reliability Analysis (HRA)

An HRA is essential in a PRA to identify and evaluate those human actions relevant to the accident scenarios being analyzed. Given the high degree of hardware reliability and redundancy, human interfaces become a critical aspect in causing, preventing and mitigating an accident. In fact, human errors have been shown to be important contributors to the frequency of core damage and the potential for a large early release. Appropriate modeling of such human actions in the baseline PRA and in specific risk-informed applications is thus critical.

2.1.5.1 Considerations for the Baseline HRA

Key factors to consider in reviewing (or supplementing or refining) portions of a baseline PRA include: selecting a human reliability analysis model, selecting human events to model, screening/excluding human events, evaluating and quantifying human events, integrating HRA into sequence quantification, and documenting the work. Each of these areas is discussed below.

Selecting HRA Model/Method

Several HRA methods (including data bases) are available to evaluate and estimate the probabilities of human events (Ref. 2.12). The strengths and weaknesses of each method should be considered, and the model/method most appropriate to the human events and situations being analyzed should be selected. Therefore, the model/method selected has certain inherent characteristics (as described below).

Identifying and Selecting Human Events

Generally, a baseline HRA identifies and quantifies relevant errors of omission (errors involving failure to correctly initiate a specific action). Currently, methods to address errors of commission (errors involving unintended actions) have not sufficiently evolved to the point that they are typically included in PRAs. The relevant errors of omission that are included in a baseline PRA are those human actions that can cause a system or component to be unavailable when demanded (referred to as pre-initiators), and those human actions needed to prevent or mitigate core damage given the initiator has occurred (referred to as post-initiators).

A PRA considers pre-initiator human events that could result in an unrevealed unavailability of a standby system or component. At a minimum, these events include restoration errors in returning the system and components to their normal state after completion of testing and maintenance, and miscalibration errors of critical instrumentation (both independent errors and common-cause miscalibration where appropriate).

Events should be included that represent:

- failure to restore equipment to correct standby status as a result of carrying out tests in which the equipment required to respond to an initiating event is realigned away from its required position, and for which the demand signal is bypassed or defeated (e.g., testing of SLC system in BWRs)
- failure to realign those components (typically valves) which, for the execution of maintenance acts, are required to be realigned away from their normal positions, and are either manually operated, or power operated with power removed or automatic realignment disabled.
- sensors which if miscalibrated could cause failure of a required system to initiate or realign e.g., steam generator level sensors.

A PRA should consider both 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 emergency operating procedures). Human response actions that are included in a PRA are those actions required to manually initiate, operate, control or terminate those system and components needed to prevent or mitigate core damage. The modeled response actions include those action needed to ensure that the systems or components meet the requirements of the success criteria defined for those systems or components in the systems analysis.

Recovery actions include those human actions performed in *recovering* a failed or unavailable system or component. Recovery actions may also include using systems in relatively unusual ways. However, credit for recovery actions may not be given unless at least some procedural guidance is provided or operators receive frequent training that would lead them to perform the required actions. Recovery actions can also include restoration and repair of failed equipment (i.e., hardware failure). Generally, restoration and repair of (LOOP), loss of PCS, loss of diesel generators and loss of DC buses have been credited. These are usually treated by using actuarial data rather than by HRA methods. Table 8.2-10 of NUREG/CR-4550, Volume 1 (Ref. 2.13) provides acceptable values for these events. NSAC-188 (Ref. 2.10) or a later NSAC report such as NSAC-194 is also an acceptable source of data for restoration of offsite power. Due to the general lack of acceptable data, restoration and repair of other equipment is generally not credited in a PRA.

The human events selected for evaluation in a PRA reflect the actual operating and maintenance practices of the plant. At a minimum, plant walk-throughs, interviews with plant personnel (e.g., training, maintenance, operators, shift supervisor, shift technical advisors), and procedure review are performed in identifying and selecting the human events for a PRA. Observation of simulator exercises of the modeled accident sequences can be used to provide additional information regarding control room operational practices and crew performance. Similarly, observations of maintenance crew performance can also be made.

The HRA should address both the "diagnosis" and "execution" portion of each post-initiator human event. Diagnosis is usually assumed to include detecting and evaluating a changed or changing condition and then deciding what response is required. Obviously, the complexity can vary, but a diagnosis may entail no more than detecting an indication in the control room and deciding to execute a prescribed response according to symptom-based emergency operating procedures (EOPs). Evaluation of the execution of a human action entails examining the activities to be conducted as indicated by the diagnosis.

2 Level 1 PRA Modeling for Fullpower Operations

In a PRA, post-initiator human events are generally assumed to entail a diagnosis phase. Exceptions to evaluating a diagnosis phase include those instances when the diagnosis of a previously modeled human event can be shown to include that for a subsequent event.

Failure to explicitly model and evaluate the execution of a human action is appropriate when the HRA method being used stipulates that the likelihood of potential execution failures is included in the diagnosis value for certain kinds of events. However, relatively complex actions may not be contained within the diagnosis value (e.g., unusual actions performed outside the control room). The application of any HRA method requires the analyst to ensure that the assumptions and characteristics of the method are appropriate for the event being analyzed. Most existing methods provide alternatives for treatment of different types of events.

Screening/Excluding Human Events

There are numerous human events that do not play a "critical" role in initiating, preventing, or mitigating core damage. A screening analysis can be performed to identify and exclude these events from detailed evaluation. However, the screened human events should be reconsidered for every risk-informed regulatory application of the PRA to ensure that all of the risk contributing actions are included in the application analysis.

Human events, such as all pre-initiators, generally cannot be excluded from consideration based on the argument that these events are included in the component hardware data. Many human events (such as miscalibration) occur rarely and are not necessarily reflected in the random failure data. Further, their effects can be subtle in that they impact multiple systems and thus can play a key factor in contributing to core damage.

In screening human events, the following criteria can be used:

- if the components that are reconfigured are misaligned but not disabled and would receive a realignment signal on system demand, events associated with realignment of the components can be screened out. (This is already embedded in the selection criteria suggested above.)
- if the activity is a maintenance activity and a full functional test is carried out on completion of maintenance, misalignment of components can be screened out.
- if the status of reconfigured components is indicated in the control room, and the expected frequency of reconfiguration is low, compared to the frequency of status checking, the failure to restore can be screened out.
- quantitative screening values for post-initiator human errors are typically used in the initial PRA quantification process when the human events are modeled in the event trees as top events or in the fault trees. The screening values assigned should be high enough to ensure that the impact of dependencies between events are not underestimated. If screening values are too low and potential dependencies are not considered, important sequences may be truncated. If screening values are assigned before the initial quantification without any examination of the events and potential dependencies, screening values not less than 0.5 (assuming that cutset truncation values around $1E-9/ry$ are used in the quantification process) are recommended for post-initiator human events.

In the final quantification step, if screening values remain for any of the human events, care should be taken so that this situation does not distort the results. Screening values, by definition, are relatively high probabilities, and when mixed with human events of more realistic values, could erroneously "drive" the results. That is, a sequence could become dominant because it included a human event with a screening value that did not properly represent the actual "reliability" of the operator. Following the initial quantification, all the human events not in the truncated sequences and cutsets, should be quantified with a detailed HRA model in order to bring the true significance of human actions to the final results.

Evaluating and Quantifying Human Events

The actual performance of the operators is reflected in the estimated likelihood of an operator failing to diagnose, perform or properly execute the needed action. Therefore, the quantification of the human events, in a PRA, incorporates plant-specific factors and practices. These factors include the following:

- Plant "conditions" affecting operator performance including:
 - The quality (type and frequency of training) of the operator training, the written procedures and of the administrative controls.
 - The environment (e.g., lighting, heat, radiation) under which the operator is working.
 - The accessibility of the equipment requiring manipulation.
 - The necessity, adequacy and availability of special tools, parts, clothing, etc.
 - The quality of the human-machine interface.
 - The availability of instrumentation needed to take corrective actions.
- The time available to the operator to determine and perform the desired action, compared with time that is actually needed to determine and perform the action. The available time is accident sequence specific and determined from engineering analysis which include actual time measurements derived from walk-throughs and simulator observation. The point at which the operators receive relevant indicators is also considered in determining available time. Thermal-hydraulic calculations can be used to help determine the time available for performing required actions.
- Task characteristics such as the number of subtasks and their complexity.
- The potential for additional checks (e.g., due to indication of changing plant parameters) on operator actions (immediate recoveries) and the expected arrival of additional support such as an emergency response team.
- Dependencies and interfaces between the human events and their relationship to the accident scenario including the following:
 - For pre-initiators, the capability of the operator to impact more than one component, train or system, is considered. (For example, the likelihood of the operator miscalibrating all level and pressure instrumentation simultaneously should be considered.)
 - For post-initiators, the human event is evaluated relative to the specific context of the accident progression. Therefore, for different accident sequences, the human event is evaluated for each sequence. The influence of previous human actions and system performance are considered relative

2 Level 1 PRA Modeling for Fullpower Operations

to their influence on the human event under consideration. Time dependency is also considered in the sense that the total available time should be considered across the entire sequence. For example, if most the total time available is allocated to the first operator action in a sequence, then the potential success of remaining actions is impacted.

The following criteria can be used to help ensure that no dependencies exists between human events (i.e. the events are truly independent).

- No common "environmental" factors exists (lighting, temperature, etc.)
- No common human-related factors exists (e.g., same/similar procedure, common-cues, same crew performing multiple calibrations on the same day, etc.)

Different personnel are involved in diagnosing and executing the human action or series of human actions.

Errors made in performance by the original operator can be "recovered" by the same operator (e.g., new plant status information) and by other plant personnel (e.g., post maintenance verification by a separate operator, role of shift technical advisor, role of emergency response team). Total credit for all such "recoveries" should not exceed a factor of 10 (higher credits should be identified and justified). This suggested limit is based on the uncertainty associated with determining the actual independence of the plant personnel and the ability to precisely quantify human performance, particularly considering all the different uncertainties.

Operators can perform numerous activities during an accident to prevent core damage from occurring. However, the likelihood of these actions can become questionable if too many or unrealistic operator actions are modeled. While all reasonable actions for which time is available can be modeled, it is recognized that an operator or control room failure in one instance (e.g., failure to follow procedure) has the potential to influence the likelihood of later operator success. Thus, potential dependencies should be considered and it is recommended that for a given cutset, the total "crew" (both control room and ex-control room operators plus any and all other personnel such as the emergency response team) failure probability be bounded to reflect resource limitations and other uncertain factors.

The above factors are used in determining what data are selected from the various HRA methods in deriving the actual human error probabilities (HEPs). The quantified HEPs are characterized as dictated in the selected HRA method. For example, the Technique for Human Error Rate Prediction (THERP) characterizes data as median values with a log normal distribution. However, the values input into the sequence quantification should be mean values, therefore, depending on the HRA method being used, conversion to a mean might be necessary. Furthermore, the associated distribution can potentially result in a portion of it being greater than 1.0 (e.g., HEP mean value of 0.8 with an error factor of 15 will result in the 95% confidence limit being greater than 1.0). In such cases, modification of the distribution is required. An acceptable approach is the use of the maximum entropy distribution which sets both the upper and lower limits.

An essential aspect in the quantification of the human events is a "sanity" check of the HEPs. The analyst should review the final HEPs relative to each other to check their reasonableness given the plant history and operational practices and experience. For example, the human events with the relatively higher failure probabilities are generally events involving more complex, difficult activities that are performed under more burdensome, time constrained and stressful circumstances. The human events with the relatively lower failure probabilities are generally events performed under more common, routine and straightforward circumstances.

Integrating HRA Into Sequence Quantification

The human events in a PRA are integrated into the overall model using several methods. Pre-initiator human events are included directly in the system fault trees where the process of model quantification accounts for human error impact on the results. However, post-initiator human errors can be modeled as a top event in the accident sequences development (e.g., event trees), as a basic event in the fault trees, and/or incorporated directly into the cutsets. However post-initiator events are incorporated into the models, care should be taken so that the actual human error probability used in the quantification process addresses dependencies between operator actions, sequence timing, and the other factors influencing the HEP. The attributes for this incorporation are provided in Section 2.1.6.

2.1.5.2 Application Impact Considerations

It is possible that a particular change to a plant's CLB may influence the HRA models and results. Proper use of a PRA in a risk-informed regulatory application requires that the impacts of proposed plant or procedural changes be included in the PRA. The actual nature of impact will be application specific. However, in general, the proposed change should be evaluated for the impact on the following HRA considerations:

- The appropriateness of the selected HRA methodology.
- Identify if any new human event may occur as a result of the CLB change. Alternatively, determine if an existing human action modeled in the baseline PRA is no longer of concern due to the CLB change.
- Review the human actions excluded in the baseline PRA to ensure the exclusion is still appropriate for the CLB change evaluation.
- Identify if the CLB change would impact any factor used in quantifying the baseline PRA human events and modify the quantification as appropriate.
- Identify if the CLB change would impact human events included in the evaluation of the containment performance during a severe accident.

2.1.5.3 Interfaces with Other Tasks

The HRA portion of a PRA interfaces with several other PRA tasks. Beginning with the initiating event task, the HRA may be used to support the identification of human-related initiating events. The HRA task also identifies the human events to be included in the plant logic model (i.e., the human error events included in the event tree structure) and in the systems models (both pre-accident human errors and response actions). The quantification of post-accident human error probabilities is performed within the context of the accident sequence cutsets and thus can only be performed after a preliminary quantification of the PRA model provides the combination of events and their timing that result in core damage.

The HRA also provides support to the Level 2 portion of a PRA. Human actions required to mitigate a core damage accident and prevent a release can be evaluated using the same techniques used in the Level 1 analysis.

2 Level 1 PRA Modeling for Fullpower Operations

2.1.5.4 Documentation

The documentation of an HRA should be sufficient that a peer reviewer can reproduce the results. At a minimum, the following information pertinent to the baseline HRA should be documented. In addition, modifications to baseline HRA should be documented for each CLB change application evaluation.

- A list or general description of the plant information that was used in the HRA.
- A list of all human actions evaluated (both pre- and post-initiator).
- A list of all HEPs for each human action.
- A list of factors used in the quantification of the human actions, how they were derived (their bases), and how they were incorporated into the quantification process:
 - time available versus time required
 - dependencies
 - plant-specific PSFs
 - diagnosis and execution.
- Source of data used to quantify human actions.
- Screening values and their bases.
- Any assumptions that were made in the human reliability analysis, as well as the bases for the assumptions and their impact on the final results.

2.1.6 Accident Sequence Quantification

The model results include point estimates, as well as results of uncertainty analyses and appropriate importance measures and sensitivity analyses, to the extent that these provide additional insights and confidence in the results³. Factors important to the accident sequence quantification task are discussed in this section.

2.1.6.1 Considerations for the Baseline PRA

Selecting the Quantification Model/Code

Several accepted computer codes are available to perform the quantification; however, the computer code actually used should be benchmarked. The computer codes can use the rare event approximation when event probabilities are below 0.1. However, use of the minimal cutset upper bound is always suggested as a minimum to avoid overly pessimistic results. The code should be capable of accounting for system successes in addition to system failures in the evaluation of accident sequence cutsets. This can be accomplished using either complimentary logic or a delete term

³The use of importance measures is provided in Appendix A.

approximation used in many existing codes. In either case, success probabilities of equipment failures and human errors are used in the computation when the probability is not close to 1.0.

Initial sequence quantification can be performed using point estimates. The values used for the point estimates are the mean values of the probability distributions for the basic event failure probabilities. As previously indicated, in Section 2.1.5, when screening values are used for post-initiator human error probabilities during the initial quantification, they should be selected to ensure that no potentially important accident sequence cutsets are eliminated. Cutsets generated from the initial quantification should be reviewed to eliminate invalid cutsets. Final quantification should be performed to replace the post-initiator human screening values with appropriate human error values as discussed subsequently.

Selecting Truncation Values

Truncation is an iterative process of eliminating accident sequences and cutsets from further consideration, based on low frequency of occurrence. This truncation is done to simplify the quantification process and make it less time intensive. Truncation is generally performed at a cutset level during the evaluation of each accident sequence where all cutsets of a frequency less than the selected truncation limit are eliminated. Cutset truncation based on the order of the cutset is not performed because cutset order is independent of the quantitative significance of the cutset.

Sequences with low frequencies can be truncated in either the initial or final quantification process, but the truncation should be performed to avoid missing any accident sequences that significantly contribute to the model estimation of total core damage frequency. At least 95% of the total core damage frequency and 95% of the early and late release frequencies should be expressed in the model results. Also, it should be verified that lowering the truncation limit does not significantly increase the model estimation of total core damage and release frequencies.

Truncation has to be considered both before and after operator recovery actions are applied to avoid discarding important sequences. The final truncation limits can be established by an iterative process of demonstrating that the overall model results are not significantly changed and that no important accident sequences are inadvertently eliminated. As a guide, a truncation value that is four orders of magnitude lower than the final CDF is usually sufficient. Note that the process of quantification including truncation, should be performed for each risk-informed regulatory application of the PRA since the impact of the regulatory change can potentially impact which cutsets and sequences can and cannot be truncated.

Integrating HRA Into the Quantification Process

Besides the incorporation of human error events directly into the event or fault tree models, events depicting the non-recovery probability of proceduralized (or otherwise expected) human actions to mitigate an accident sequence should be added during the quantification phase of the analysis. The number of operator recovery actions added to an accident sequence should be limited to "reasonably expected" operator actions. Reasonably expected means that the operator actions are specified in procedures and do not consist of heroic type actions. Also, as discussed in the previous section, the total credit of post-initiator human actions for a given sequence or cutset should be reasonably bounded (e.g., not less than $1.E-6/ry$).

Regardless of the type of human error, care should be taken to identify dependencies among multiple human error events which occur in individual cutsets so that the combined human error probability is not optimistically evaluated. This implies that cutset-specific timing and conditional information should be used in the calculation and application

2 Level 1 PRA Modeling for Fullpower Operations

of post-initiator operator actions and other recovery actions. Application of such actions at a sequence level cannot generally be performed.

Estimating Uncertainties

The use of PRA in risk-informed regulation should take into account the potential uncertainties that exist so that an estimate can be made of the confidence level applied to the quantitative results obtained for a particular application. The mean values obtained from the PRA are used in the decision making process. Use of the mean value in the decision making process does not, however, resolve the need to quantify (to the extent reasonable) and understand those important uncertainties involved in the PRA and particularly in the risk-informed regulatory application of the PRA.

There are two general types of uncertainty. "Parameter uncertainty" results from the lack of knowledge about the input failure rates used in the models. "Model uncertainty" occurs when alternate models can be constructed to represent the accident sequence behavior. (This includes concerns about the model completely representing all significant phenomena).

Parameter uncertainty should be incorporated into the model. This involves propagation of the failure rate distributions calculated in the data analysis task through the PRA models. Events in the PRA representing the same component failure with the same failure rate are correlated in the uncertainty analysis (correlation can dramatically affect the resulting core damage frequency uncertainty distribution). To the extent practical, modeling uncertainty should also be incorporated into the PRA. This can involve applying weights to different models and propagating the impacts of these models through the entire PRA. An alternative is to perform sensitivity analyses to determine the impact of the different models.

Acceptable methods for performing uncertainty analysis include Monte Carlo simulation or the variation known as Latin Hypercube Sampling. Equivalent means of propagating uncertainties may also be used. The computer codes used for the uncertainty analysis should have been benchmarked to verify that the results provided are reasonable. An uncertainty analysis should be performed for each risk-informed regulatory application of the PRA using the retained accident sequences (i.e., the sequences reflecting 95% of the CDF and 95% of the early and late release frequencies). In addition, the uncertainty analysis should be performed using a large enough sample to demonstrate convergence of the results.

Computing Importance Measures and Performing Sensitivities

The sensitivity of the model results to model boundary conditions and other key assumptions should be evaluated using sensitivity analyses to look at key assumptions or parameters both individually or in logical combinations. The combinations analyzed should be chosen such that interactions among the variables affected by the sensitivities are fully accounted for. Areas typically needing evaluation using a sensitivity analysis are modeling assumptions, human error probabilities, common cause failure probabilities, and safety function success criteria. The results of these sensitivity analyses are needed to provide some confidence in the PRA results particularly as applied to risk-informed regulatory applications.

In performing sensitivity analyses, the analyses should not be performed by manipulating (requantifying) the "retained" accident sequences and cutsets. The sequences and cutsets that were truncated could potentially be impacted and significantly influence the results (e.g., dominant accident sequences and contributors). Therefore, the sensitivity

analyses should be performed by requantifying the entire PRA model unless it can be shown that only the retained accident sequences and cutsets are impacted.

Importance measure calculations should be performed to provide information regarding the contributions of various components and basic events to the model estimation of total core damage frequency. Typical importance measures are Fussell-Vesely, risk achievement, risk reduction, and Birnbaum. The definition and use of importance measures are discussed in Appendix A.

2.1.6.2 Applications Impact Considerations

It is quite likely that proposed changes to the CLB will impact the results of this task. The proposed changes should be reviewed to determine if they result in:

- Previously truncated cutsets becoming important.
- Reordering of sequences based on their importance.
- Changes in the uncertainty analysis.
- A need for additional sensitivity analyses to be performed.
- Changing in results of importance analyses.
- Different operator recovery actions.

2.1.6.3 Interfaces with Other Tasks

The systems analysis task may provide information needed to debug the quantification task (e.g., explain why certain cutsets exist, or show where errors were made in modeling). The data analysis task will provide input data for the model to be quantified. The sequence analysis task provides the framework for the model which is quantified. The output of the quantification task (e.g., the cutsets) can be used to find any errors in the modeling of other tasks. It is also used to provide insights about the plant's risk profile.

2.1.6.4 Documentation

The following information regarding the PRA quantification should be documented:

- A general description of the quantification process including accounting for systems successes, the truncation values used, how recovery and post-initiator human errors are applied, and a description of the computer codes used.
- The total plant CDF and contributions from the different initiating events and accident classes.
- A list of the dominant accident sequences and their contributing cutsets. (A dominant accident sequence, from a frequency perspective, rather than a risk perspective, is defined here as one whose contribution to the total CDF is greater than 1%.)
- Equipment or human actions that are the key factors in causing the accidents to be non-dominant.
- The results of all sensitivity studies.

2 Level 1 PRA Modeling for Fullpower Operations

- The uncertainty distribution for the total CDF and for each dominant accident sequence.
- Importance measure results, including at least Fussell-Vesely, risk reduction, and risk achievement.
- A list of mutually exclusive events eliminated from the resulting cutsets and their bases for elimination.
- A list of all sequences retained after the final quantification, including a brief description of the sequence and its CDF.
- Records of the actual quantification process such as file manipulations, setting of flags to turn portions of logic either on or off, etc.
- Records of the process/results when adding non-recovery terms as part of the final quantification.
- Records of the cutset review process and any manipulations therein such as eliminating invalid cutsets, requantifying multiple but dependent human errors in the same cutset, etc.

2.2 Internal Flooding Analysis

While the internal flooding analysis of a PRA uses much the same processes and has the same attributes of a traditional full power internal events PRA (Section 2.1.1), the internal flooding analysis requires a significant amount of work to define and screen the most important flood sources and possible scenarios for further evaluation.

The major tasks associated with the Level 1 portion of an internal flooding analysis include:

- Flood source and propagation pathway identification and screening
- Flood scenario identification and screening
- Flooding model development and quantification.

The information developed during the flooding source and propagation pathway identification and screening task is used to identify and quantify the flood scenarios. Results from the identification and quantification of the flooding scenarios are then used in the flooding model development and quantification task. While analogous to the initiating event identification and exclusion portions of the full power internal events PRA, the first two tasks require consideration of different plant characteristics with particular emphasis on the spatial aspects of the plant's design. Consideration of structures, barriers, drainage designs, and different failure modes (e.g., water submersion of equipment, water spray on electrical equipment) are examples of aspects of the plant that should be considered in the internal flooding analysis that are not necessarily addressed in the traditional internal events analysis. After the flooding scenarios have been screened for detailed quantification, the third task follows much of the modeling and quantification aspects already carried out in the internal events analysis with relatively minor modification.

Three scoping attributes should be met to better ensure completeness of the analysis. First, a PRA should consider not only floods as initiating events, but also include the possibility of flooding occurring as a subsequent event to some other initiator. Second, both water and steam source effects (i.e., jet impingement, splashing, submersion, pipe whip, and condensation) should be considered. Finally, flooding induced by both equipment failure as well as human-induced events (such as failure to properly isolate a potential flood source before doing maintenance) should be

examined. Attributes that are unique to the internal flooding analysis (compared to the internal events analysis) are addressed below.

2.2.1 Considerations for the Baseline PRA

2.2.1.1 Identification and Screening of Flood Sources, Propagation Pathways, and Flood Scenarios

The first two tasks identified above are performed together in a somewhat iterative manner because there are numerous interactions between the tasks. The guidance provided in NUREG/CR-4832 (Ref. 2.14) can be used for performing the specific steps necessary to identify and screen the flood scenarios. These specific steps are not reproduced here; however, certain overriding attributes that should be met in performing a sound baseline internal flooding analysis are highlighted below.

All substantial water and steam sources should be carefully screened. As a minimum, possible sources should include piping, valves, pumps, tanks, heat exchangers, room coolers, chillers, fire suppression systems (including both inadvertent actuation and piping failures), relief valves, potentially large bodies of water in the plant (such as the suppression pool in BWRs and the spent fuel pool), and nearby reservoirs, lakes, rivers, and oceans that are connected to the plant through some plant systems or structures (such as the ultimate heat sink that is connected to the plant through service water system). Any qualitative arguments used to screen or otherwise eliminate flood sources (e.g., small size, location arguments, effects are similar and greater for another flood source, etc.) should be well documented and based on sound engineering principles and judgment. While probabilistic arguments can be used at this stage, they should meet the initiating event exclusion principles provided in Section 2.1.1. Both leakage and rupture failure modes should be considered as well as the potential for human-induced flooding.

Sources and locations of concern (particularly the identification of propagation pathways) should be supported by actual walkdowns of the plant. Flood zone definitions should consider the existence of barriers and drains that can confine the flood to an area. Propagation paths from one flood zone to another should consider stairways, doorways, hatches, floor and wall penetrations and cracks, drain lines, HVAC ducts, piping/conduits, etc., and should consider the potential failure of barriers to propagation (e.g., normally closed door failing open once the flood water reaches a certain height behind the door). Any assumptions or other judgment used to define and screen out possible locations and pathways should be documented and based on analyses, calculations, or sound engineering judgment. Isolation arguments should consider methods of detection, access, and available means to isolate or otherwise mitigate the flood source, and the time to carry out appropriate actions. In addition, the availability of other flood mitigation systems or actions such as drain lines or sump pumps need to consider sizing and the potential for plugging. With regard to determining possible flowrates, the analyst should consider whether forced flow (such as from an active pump) or passive flowrates are expected.

The above information leads to the formulation of possible flood scenarios that should be considered. These scenarios are more completely defined by considering what (and how) equipment is affected in the context of the possible accident sequences that can lead to core damage (as indicated by the internal events analysis). It is therefore important that the possible flood-induced failure modes (i.e., susceptibility) of equipment be considered besides the random failures of equipment covered in the internal events analysis. Any guidance used in the flooding analysis with regard to the failure modes to be considered should be clearly defined and have a reasonable basis. For instance, electrical equipment (buses, motor control centers, batteries, inverters, motors for valves and pumps and fans, etc.), if submerged, or exposed to a high steam environment should be assumed to short-out and therefore be unable to operate, at least during the screening steps conducted in the analysis. Mechanical equipment may be considered to fail under

2 Level 1 PRA Modeling for Fullpower Operations

special circumstances such as when HVAC ducting is flooded and fails because of the water weight and so on. Screening of potential accident sequences on the basis of what equipment is or is not affected, as well as consideration of the above failure modes, should be clearly identified and supported.

2.2.1.2 Flooding Model Development and Quantification

With some modifications, the modeling of the resulting unscreened scenarios uses many of the same sequence models (typically event trees) and system failure models (fault trees) used in the traditional internal events analysis. The mitigating system fault trees should be modified to account for possible combinations of flood-induced as well as random failures of equipment. The types of initiating events resulting from internal floods should include not only transients but also LOCAs induced through spurious valve operation. As stated earlier, consideration should be given to both floods as initiators as well as floods that occur during or as a result of some other transient. Also, the potential for multiple initiating events should be reviewed. The internal event trees can generally be used in a flood analysis but should also reflect additional mitigating systems and actions as appropriate.

The quantification portion of the analysis is essentially the same as described in Section 2.1.6 but should recognize the potential for new or more severe PSFs when considering human failure probabilities and possible recovery actions. However, an initial bounding quantification can be performed using pessimistic assumptions on flood propagation and equipment susceptibility. Flooding scenarios that survive such bounding assessments should be requantified using refined estimates of the flooding impacts (obtained through engineering analysis) to provide a realistic analysis.

2.2.2 Application Impact Considerations

In general, the application impact considerations that impact the internal event models identified in Section 2.1 are applicable here. In addition, application impacts on the flooding-specific portions of the analysis also need to be addressed. For example, if an application has the potential of increasing the failure probability associated with piping, then the screening performed as part of the original flooding analysis should be reexamined to determine what impact the new failure probability has on the screened scenarios. Areas that should be reviewed include:

- The potential for the introduction of a new flooding source or the removal of an existing flood source.
- The potential for changing the flood propagation potential for an existing or new flood source.
- The mitigation of a flood source (e.g., isolation) may possibly be affected and should be reviewed.
- The impact of a flooding event on accident mitigating equipment may be altered by a plant modification and should be reviewed.
- The potential for new or additional initiating events resulting from plant modification and impacts on the models used in the accident sequence quantification (i.e., event trees, fault trees, and HRA) should also be reviewed.

2.2.3 Interface with Other Tasks

This task uses extensively the information gathered and models developed in the internal event analysis. In particular, the fault trees and event trees developed for internal events are modified and used for modeling floods.

2.2.4 Documentation

The process of identifying flood sources, flood pathways, flood scenarios, and their screening, and internal flood model development and quantification should be documented for both the baseline PRA and any modifications made in analyzing a modification to the plant CLB. In addition to the information normally documented in a traditional internal events analysis, at a minimum, the following information should be documented for an internal flooding analysis:

- a definition of the flood zones used in the analysis and the reason for eliminating any of these areas from further analysis.
- a list of flood sources considered in the analysis and any rules used to eliminate these sources.
- a discussion on the propagation pathways between flood zones and any assumptions, calculations, or other bases for eliminating any of these propagation pathways.
- a listing of accident mitigating equipment located in each flood zone not screened from further analysis.
- a list of any assumptions concerning the impacts of submergence, spray, temperature, or other flood-induced effects on equipment operability.
- a discussion of how the internal event analysis models were modified for the internal flooding analysis.
- a list of the flood frequencies and component failure probabilities from flood effects and their bases, and
- a discussion of any calculations or other analyses used to refine the flooding evaluation.

2.3 Internal Fire Analysis

A full power internal fire PRA utilizes the same overall analysis approach and procedures used in performing a full power traditional internal events PRA (Section 2.1). In fact, there are many points of commonality between the traditional internal events analysis and an internal fire risk analysis. These include the use of the same fundamental plant systems models (event trees and fault trees), similar treatment for random failures and equipment unavailability factors, similar methods of overall risk and uncertainty quantification, and similar methods for the plant recovery and human factors analysis. Consistency of treatment of these commonalities is an important feature in a fire risk analysis. It is also important that the documentation of an internal fire risk analysis parallel that of a traditional internal events PRA, with supplemental documentation of the unique fire related aspects of the analysis provided as necessary.

Although the overall evaluation process is the same, there are differences in the events postulated to occur in response to an internal fire event as compared to those from a traditional internal event. These unique features should be

2 Level 1 PRA Modeling for Fullpower Operations

accounted for in a sound baseline fire risk analysis. The main differences between a traditional internal events analysis and an internal fire analysis are as follows:

- Physical Plant Partitioning - physical partitioning of the plant into fire analysis areas and zones
- Equipment Identification and Mapping - identification of plant components not typically considered in an internal events analysis, including in particular electrical power, instrumentation, and control cables, and the mapping of such equipment to specific locations
- Fire Source Identification and Quantification - identification of ignition sources and quantification of their frequency
- Fire Growth and Spread Quantification - determination of fire growth and spread
- Fire Damage Assessment - the assessment of fire-induced damage to plant equipment
- Fire Detection and Suppression - determination of the effectiveness of fire detection and suppression
- Human Intervention and Plant Recovery - identification of the impact of a fire event on the possibility and likelihood of post-fire human actions (including the impact of contradictory or failed indication).

The major analysis elements described in Section 2.1 for a traditional internal events analysis are also applicable to an internal fire analysis. Differences that arise come from the fact that the fire analysis has to account for the effects of the fire and should provide for the specific treatment of the actual fire phenomena associated with the postulated fire event as presented above. A fire analysis generally consists of three phases:

- initial area screening
- secondary area screening, and
- detailed analysis.

The initial area screening phase of the analysis identifies the limited subset of plant fire areas which should be considered for more detailed analysis. This initial screening is based on consideration of the nature of the components/systems located within a fire area without specific consideration of the phenomena involved in the fire growth and damage processes. The components located within a given fire area are identified and the impact of their failures on plant systems are assessed to determine the potential for a fire in the fire area to represent an initiating event.

The secondary area screening phase is then applied to further refine the areas requiring detailed quantification by inclusion of a rudimentary treatment of the fire phenomena. This secondary screening process may be performed at progressive levels of detail. Initially, the secondary screening analysis includes a high estimate of the total fire frequency from all fire sources in a particular area, with the further assumption that all fires would result in damage to all equipment in the affected area with a probability of 1.0. If the resulting fire risk estimate falls below the specified truncation value, then the area requires no further consideration. If an area cannot be truncated on this basis, then further screening can be applied in which low estimates of fire intervention factors are introduced. However, as the analysis becomes more refined, the level of detail considered should also become more refined, resulting in the "blurring" of the "line" between a secondary screening analysis and a detailed area quantification (see next paragraph).

For example, if some credit for successful fire suppression before critical fire damage is to be given, then the analysis should include consideration of physical factors which might make it unrealistic to assume that intervention would be successful. A typical example of this would be a case in which a critical cable was located directly above an energetic potential fire source such as a switchgear cabinet such that if the fire were to be ignited, then damage would occur in a very short time.

For the subset of fire areas which survive the initial and secondary screening phases of the analysis, a detailed quantification of the fire risk for each fire source postulated to exist in that fire area is performed. Generally, at this point in the analysis, the fire areas defined in the screening analyses are further partitioned into fire zones for detailed quantification. This partitioning essentially results in the definition of what specific components are considered to be threatened by a fire event.

As part of each phase in a fire PRA, the potential effects of a fire within a single fire area or zone and the effects of inter-area and inter-zonal considerations (i.e., the effects of multiple fire areas or fire zones in combination to represent significant contributors to fire risk) are determined. The assessment of the potential that a fire in one fire area or zone might impact equipment in an adjacent fire area or zone is particularly important for the high hazard fire areas (in which a fire might threaten even a three-hour rated boundary), zones bounded by fire barriers of less than three-hour rating, and fire areas or zones separated by active fire barrier elements (such as normally open fire doors, water curtains, ventilation dampers, etc.). Consideration should be given to the likelihood that fire barrier penetration seals might fail under certain types of fire conditions (such as larger fires or fires immediately proximate to the seals).

Within each of the assessment phases, the fire-specific differences between a traditional internal events analysis and an internal fire analysis should be dealt with. The level of detail applied to the assessment of each of these specific differences depends largely on the phase of the fire analysis. That is, the screening phases may include only a rudimentary treatment of certain differences, whereas the detailed quantification phase will require a specific and comprehensive treatment of each difference. Attributes for each specific difference are presented in the following sections. In addition, fire-unique attributes for each of the PRA analytical tasks identified in Section 2.1 are provided.

2.3.1 Considerations for the Baseline PRA

This section provides the attributes of a detailed fire PRA that could be utilized as the base model in the evaluation of a CLB modification. The fire-specific aspects of the PRA are discussed as well as the interfaces with the internal event PRA models.

2.3.1.1 Defining Fire Areas or Fire Zones

Since the physical partitioning of the plant effectively defines which components and systems will be considered simultaneously vulnerable to a common fire event (with the exception of the final inter-area or inter-zonal fire analysis stage), the partitioning process significantly impacts the final analysis results.

The terms *fire area* and *fire zone* are widely used in fire risk assessment and are also recognized terms with specific definitions in the context of fire protection. A *fire area* is generally defined in the fire protection context as a physical region which is fully bounded by three-hour rated fire barrier systems (as certified by the ASTM E119 fire performance test). The above traditional fire protection community definition of a fire area is consistently applied in fire risk analyses, but it should be recognized that the term *fire zone* can represent many different levels of physical separation. That is, the term *fire zone* has a more flexible and judgmental definition, and is generally associated with any physical

2 Level 1 PRA Modeling for Fullpower Operations

region bounded by lesser fire barrier elements. In some cases, fire zones can be defined in risk assessments as regions with no specific physical boundary elements which are nonetheless considered to represent the physical limits of influence for any fire in that region. For example, a multi-level fire area separated by floor/ceilings with open equipment hatches might be defined for the purposes of analysis as several separate fire zones despite the presence of an open pathway between the zones. Similarly, a physical region of twenty feet of horizontal separation with no intervening combustibles (an Appendix R provision) can be cited as defining the limit of a fire zone despite the lack of any physical barrier between adjacent fire zones. Since there is flexibility in the definition of a fire zone, a fire analysis should define each fire zone identified and used in the analysis.

With respect to the three analysis phases identified above, a fire PRA can use the following partitioning process:

- Initial area screening is based on the consideration of fire areas as traditionally defined in the fire protection context. Fire zones, as used in fire risk assessments, are not used.
- Secondary area screening is initially based on the use fire areas. As the screening becomes progressively more detailed, the use of fire zones becomes acceptable as long as such use is supported by specific and detailed consideration of the fire phenomena involved. (NOTE: This is generally inconsistent with the intent of the screening process, but is acceptable if all relevant fire phenomena are considered.)
- Detailed area quantification is based on the use of fire areas or fire zones, whichever is appropriate.

2.3.1.2 Equipment Identification and Mapping

The critical plant systems and components of interest to the analysis should be identified. This is generally based on an examination of the risk important systems considered in the traditional internal events analysis described in Section 2.1, supplemented by consideration of fire-related plant documentation such as the plant Appendix R submittal, and verified by plant walkdowns. Consideration of only the plant Appendix R systems is not an adequate basis for analysis in a fire PRA. Electrical cables (power, instrumentation, and control) for all systems and components should be included in this assessment. After identifying the equipment, the location(s) of each of the components identified should be traced to specific plant locations. This step can involve multiple levels of detail. For example, for the purposes of initial screening, mapping a piece of equipment to a specific area is sufficient. For secondary screening, mapping to fire areas or fire zones is warranted. In contrast, detailed quantification of area or zone fire risk requires that the equipment be mapped to very specific locations within the fire area or zone. This is because the area of influence of most fires will be limited to a subset of the fire area or zone, and because the proximity of the critical equipment to the fire source will directly and profoundly impact the timing of equipment damage.

2.3.1.3 Fire Source Identification and Quantification

The fire analysis should both identify possible fire sources in a given plant location, and quantify the frequency with which each of those fire source might initiate a fire event. This includes both fixed fire sources (pumps, motors, electrical panels, switchgear transformers, fuel and oil storage media, hot pipes such as diesel generator exhaust pipes, electrical cables, etc.) and transient sources (trash, maintenance activities including equipment and supplies, sources of liquid or gaseous flammable material leaks, short term storage items, long term storage items, etc.). A fire events data base is typically used to support this part of the analysis. In general, a fire analysis considers all possible fire sources. Consideration of only the single most significant or largest fire source in a given area is not generally considered an adequate basis for the analysis. This is because the fire threat is a combination of several factors and

the largest or most significant perceived fire threat may not, in fact, represent the bounding condition in the context of fire risk.

2.3.1.4 Fire Growth and Spread Quantification

The fire analysis should also quantify the potential for an initial fire source to both grow within the limits of that initial fire source and for the fire to spread to other nearby flammable materials by considering the maximum credible size (both the intensity and physical extent) associated with the initial source and the potential for that fire source to ignite other nearby materials. The analysis of fire growth within the initial fire source may be based on either a fire computer model or on available test data, but the analysis of fire spread to other nearby materials requires the application of a proven fire growth computer model of some type.

2.3.1.5 Fire Damage Analysis

Based on the fire growth analysis, a prediction is made as to how the fire will impact the environment surrounding the critical components of interest and in turn how that environment will impact the operability of those components. In a fire PRA, the timing of equipment damage is one of the two most critical factors to be determined (the second is fire detection and suppression, discussed in the next section below). In order to pass beyond the initial screening steps to final quantification, the analysis should consider not only if damage will likely occur, but also the time interval between ignition of the fire and the onset of equipment damage. This process should include the identification of both the modes or mechanisms of fire damage (typically simple heating of the component but also potentially including smoke deposition) and the threshold exposure associated with the onset of equipment damage (such as damage temperature).

2.3.1.6 Fire Detection and Suppression

In general, the quantification of fire risk involves an assessment of the competing process of fire growth and damage behavior and that of fire intervention through detection and suppression (unless it is judged that time to damage is very short). The analysis of fire detection and suppression, including the timing of these intervention mechanisms, is the second of the two most critical factors associated with a fire risk analysis. This is a multi-path process which should include consideration of both fixed systems and manual intervention (both the detection and suppression events may involve actions by either fixed fire protection systems or plant personnel). The detection and suppression analyses should be linked (detection alone is largely worthless without suppression, but suppression should be predicated on fire detection unless fire self-extinguishment is postulated), and the fire damage and fire intervention analyses should be performed on a consistent basis because comparison of fire damage times to fire intervention times is the ultimate driving force for the risk quantification. Hence, both parts of the analysis should be based on consistent treatment of the relevant fire phenomena.

In addition to the potential for the fire itself to damage the crucial equipment of interest, a fire analysis should consider the possibility that application of fire suppressants (e.g., water, Halon, or Carbon Dioxide) might also lead to supplemental equipment damage. This aspect of the analysis requires consideration of both the potential effects of the fixed fire suppression systems and the possible intervention by fire fighting personnel. The most difficult aspect of this analysis typically involves the manual intervention aspects. This is because the analysis should include consideration of fire fighting access routes, the potential for the build-up of a dense smoke layer (which would increase the likelihood of misdirected water sprays), and the level of training and pre-fire planning provided to the fire fighting personnel.

2 Level 1 PRA Modeling for Fullpower Operations

2.3.1.7 Human Intervention and Plant Recovery

The final step in quantification involves an assessment of human intervention and plant recovery following the fire event by using the same process as that used in the traditional internal events analysis. The impact of the fire on the level of operator stress, and hence, the likelihood that operators might make mistakes in the recovery process, should be considered. Second, the presence of a fire in a given area is generally assumed to prevent plant personnel from taking recovery actions which require access to or through the affected fire area until well after the fire has been extinguished. If operator initiated repairs (recovery) of equipment damaged in a fire is considered, then justification should be provided that demonstrates the operators ability to make the repairs. This analysis should also include a careful examination of the plant's alternate shutdown capability for certain plant fire scenarios (typically those involving the main control room or cable spreading rooms). This aspect of the analysis includes the consideration of potential fire-induced failures which might not be evident at the remote shutdown station(s), and the level of plant equipment and systems control which is available outside the main control room.

2.3.1.8 Fire Model Development and Quantification

The following paragraphs identify the unique fire analysis attributes associated with the PRA and quantification modification of the internal events models for use in the fire analysis.

Initiating Events

The same set of initiating events identified in the traditional internal events analysis are considered in the internal fire analysis. For example, if LOCAs are considered, then fire-induced LOCAs (i.e., spurious valve openings) should be considered. Initiating events that cannot be caused by a fire-induced equipment failure, or by potential operator responses to a fire event, can be eliminated. Note, for example, that even though fire-induced equipment damage in a given fire area or zone might not directly lead to an initiating event, the analysis should consider the potential that operators might take actions on a preventative basis to shut down the plant in the event of a significant fire, and that the postulated fire might render safe shutdown systems inoperable or unavailable. Fire-induced initiators that require fires in two noncontiguous fire areas can be eliminated from the analysis.

Accident Sequence Analysis

The analysis should include a specific treatment of each of the specific fire scenario differences which have been discussed in Sections 2.3.1.1 through 2.3.1.7. In addition, any fire-unique dependencies should be considered.

Systems Analysis

The fire PRA should include consideration of spatial dependencies for the following:

- cables (e.g., power, instrumentation, and control)—the location of the cables both to and through the fire areas/zones.
- all other components vulnerable to fire-induced damage or failure (e.g., pumps, valves actuators, motors, switches, and electrical panels).

- components not vulnerable to fire-induced damage or failure may be eliminated from the analysis (e.g., large piping is not typically included in fire risk analyses).

Fire-induced system dependencies should be considered in a fire PRA. In particular, the analysis should consider the potential for common-cause failure of multiple components/systems due to the effects of a given fire. This potential is unique from a traditional internal events analysis because the effects of a fire (e.g., heat and smoke) can travel quickly throughout a given fire area or zone, and can also extend beyond the limits of a single fire area or zone under certain circumstances. Effects which should be addressed include: smoke⁴, suppression agent effects, and temperature. If any of these can affect the performance of a component, then their impact should be considered. The fire PRA should also include consideration of direct thermal heating of components due to convective and radiative heating of targets by the fire.

For power and control cables, fire PRA should include some consideration of the three recognized potential failure modes; namely, conductor-to-ground shorts (which might result in simple loss of function or power bus failure), conductor-to-conductor shorting within a multiconductor cable (which might simulate the effects of a switch closing or cause a shorting of a power supply bus), and conductor-to-conductor shorting between adjacent cables (which might cause spurious operation of plant equipment, or cause destructive voltages to be applied to a lower voltage system). Each mode should be considered, and screening of failure modes is based on physical proximity and systems impact considerations.

Fire Modeling

Lessons learned from previous fire PRA studies indicate that caution should be exercised in areas, such as:

- Selection of cable ignition and damage criteria.
- Credit taken for in-cabinet smoke detection.
- Performance shaping factors associated with emergency HEPs, especially in a degraded environment caused by fire.
- Modeling of initiation and effectiveness of automatic suppression, and
- When "FIVE" is used to address NRC-mandated enhancements such as additional fire initiating events, proper consideration of certain passive components, thermal damage thresholds, self-ignited cable fires, earthquake induced fires, and containment fires.

⁴A potentially important mode of fire damage not usually included in a typical fire PRA is smoke damage. As research in this area matures, failures associated with smoke should be included in the fire analysis.

2 Level 1 PRA Modeling for Fullpower Operations

Data Analysis

Current sources of fire data should be used to support the fire analysis. A baseline PRA should:

- consider industry wide experience with Bayesian updating based on plant-specific experience when estimating fire frequency.
- use a current state-of-the-art fire growth code to determine the impact of fire propagation, and
- include a quantification of uncertainty associated with all critical input values.

Human Reliability Analysis (HRA)

In a fire analysis, the impact of a fire on the operator's ability to perform actions should be included in the identification and selection of the human actions. In particular, the impact of a fire on human stress levels and human reliability should be included in the HRA analysis. Further, the analysis should include the consideration of how the fire event might impact faulty indications, and operator actions which require access to or through the affected fire area (generally credit should not be given to such actions until well after the fire is presumed to be fully suppressed due to heat and smoke buildup and other related factors). The presumption that fire damaged equipment can be repaired as a part of the short-term fire recovery should be specifically justified on the basis of available repair items and plant procedures. A fire PRA should consider the possibility that manual fire detection and suppression are one possible path to fire intervention. The potential for manual fire detection and suppression should include consideration of the following issues:

Detection:

- the nature of the fire event (human caused or equipment failure related).
- for general plant areas, who is there, when are they there, and how frequently are they there (occupancy factors), and
- for the main control room, the configuration of the control room, its ventilation system, and in particular, the configuration of the ventilation system's return air handling ducts (which might significantly impact the timing of manual detection).

Suppression:

- who is on the fire brigade (operators, security staff, health, safety, general maintenance staff, etc.), their training, their equipment, and their experience facing actual fire situations,
- the time required for manual suppression (including initial response time as a function of zone, time to assemble and equip an effective fire fighting team, time to assess the fire situation, and time to actually suppress the fire), and
- collateral damage caused by application of suppressant agents, even if direct fire-induced damage was successfully mitigated.

2.3.2 Application Impact Considerations

In general, all application impact considerations identified in Section 2.1 are applicable for the internal events model used in the fire analysis. In addition, a proposed CLB change can impact the fire-specific portions of the analysis. For example, if an application has the potential of increasing the failure probability associated with a motor operated valve, then any screening performed as part of the baseline fire analysis should be reexamined to determine what impact the new failure probability has on the screened sequences.

Specific factors which should be reviewed for each application include:

- The appropriateness of the fire zones and area definitions used in the analysis and corresponding equipment mapping.
- The potential for the introduction of a new fire source (or conversely, the elimination of a fire source).
- The potential for a change in the fire growth and propagation potential.
- The potential for a change in the fire damage potential of equipment.
- Changes in the fire PRA model including the potential for different initiating events, additional spatial failure modes required in the system fault trees, and modified human event error probabilities.

2.3.3 Interface with Other Tasks

In general, the interfaces identified in Section 2.1 are also applicable here. Moreover, the applicable Level 1 internal events logic models should be identified and modified to account for fire induced damage. Fire induced accident scenarios are assigned to plant damage states similar to those used in the conventional internal event analysis. In addition, the following interfaces among fire-specific analysis tasks should be considered:

- the fire area and zone definitions will be used to identify the components can be affected by a fire.
- the affected components will impact the development of the system models.
- the fire source identification and quantification results will impact the initiating event identification and quantification task.
- results from the fire growth and spread task, the fire damage assessment task, and the fire detection and suppression task will impact the final sequence quantification, and
- information from the fire growth and spread task and fire damage assessment task will influence the human reliability analysis task.

2.3.4 Documentation

In addition to the information normally documented in a traditional internal events analysis, the following information should be reported in a fire PRA:

2 Level 1 PRA Modeling for Fullpower Operations

- A discussion of how the sub-set of initiating events relevant to the fire analysis was developed, and in particular, how the internal events set was screened for relevance to fire.
- A list or general description of the information used to develop the fire area/zone locations.
- A description of the process used to identify the fire areas/zones.
- A list and description of the identified fire areas/zones.
- A list of the cables and components considered in the analysis.
- A mapping of risk important components and systems to fire areas or zones.
- Justification for any system or component/cable for which location information was not provided.
- A list of any data bases, experimental results, plant procedures, plant experience, or analysis tools (such as fire computer models or correlations) used to support each step of the fire phenomena analysis.
- A list of (and justification for) the specific parameter values associated with the analysis of specific fire scenario factors.
- A list of the critical inputs and outputs associated with each scenario analyzed in a format sufficient to allow independent verification of the analysis results and in a level of detail appropriate to the stage of the analysis under consideration (e.g., screening versus detailed quantification).
- A specific discussion of how the HRA operator recovery analysis was "customized" or "modified" to account for the unique conditions of a fire event, including how manual fire detection and suppression factors were incorporated into the quantification of the fire growth, damage and intervention models.
- Results from the initial screening, secondary screening (if applied), and detailed quantification stages of the analysis.

REFERENCES FOR CHAPTER 2

- 2.1 D.M. Ericson, Jr. (editor), et al., "Analysis of Core Damage Frequency: Internal Events Methodology," NUREG/CR-4550, Volume 1, Revision 1, Sandia National Laboratory, January 1990.
- 2.2 W.J. Galyean, P.G. Ellison, J.A. Schroeder, "ISLOCA Research Program Final Report," EG&G Idaho Falls NUREG/CR-5928, July 31, 1993.
- 2.3 "Safety Related Motor-Operated Valve Testing and Surveillance," U.S. Nuclear Regulatory Commission, Generic Letter 89-10, June 28, 1989.
- 2.4 V. H. Ransom, et. Al., "RELAP5/MOD3 Code Manual," Volumes 1-5, NUREG/CR-5535, EGG-2596, EG&G Idaho Inc., June, 1990.
- J. C. Lin, et. Al., "TRAC-PF1/MOD2 Code Manual," Volumes 1-4, Los Alamos National Laboratory, LA-12031-M, NUREG/CR-5673, 1994.
- 2.5 USNRC, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, December 1990.
- 2.6 "Analysis of Core Damage Frequency from Internal Events: Expert Judgment Elicitation on Internal Event Issues," NUREG/CR-4550, SAND86-2084, Volume 2, April 1989.
- 2.7 USNRC, "Fault Tree Handbook," NUREG-0492, March 1980.
- 2.8 H. M. Stromberg, et al., "Common-Cause Failure Data Collection and Analysis System," INEL-94/0064, Volumes 1 through 6, Idaho National Engineering Laboratory, December 1995.
- 2.9 "Loss of Offsite Power at U.S. Nuclear Power Plants Through 1991," Nuclear Safety Analysis Center, NSAC-188, March 1992.
- 2.10 R. L. Iman and S. C. Hora, "Modeling Time to Recovery and Initiating Event Frequency for Loss of Offsite Power Incidents at Nuclear Power Plants," NUREG/CR-5032, Sandia National Laboratories, January 1988.
- 2.11 T. Morgan, G. W. Parry and C. S. Chuan, "Nuclear Plant Reliability: Data Collection and Usage Guides," EPRI/TR-100381, April 1992.
- 2.12 J. Wreathall, "HRA Modeling in IPEs: An Evaluation of Methods and Their Application," NUREG/CR-6520, Brookhaven National Laboratory, to be published.
- 2.13 Table 8.2-10, D.M. Ericson, Jr. (editor), et al., "Analysis of Core Damage Frequency: Internal Events Methodology," NUREG/CR-4550, Volume 1, Revision 1, Sandia National Laboratory, January 1990.
- 2.14 W.L. Ferrell, et al., "Analysis of the LaSalle Unit 2 Nuclear Power Plant: Risk Methods Integration and Evaluation Program (RMIEP)," NUREG/CR-4832, Volume 10, Sandia National Laboratory, October 1992.

3. INTERNAL EVENT LEVEL 2 PRA FOR FULL POWER OPERATIONS

This chapter provides attributes for performing a Level 2 probabilistic risk assessment (PRA) of a plant operating at full power. A Level 2 PRA evaluates containment response to severe accidents and determines the magnitude and timing of the radionuclide release from containment. Consequently, those PRA applications that deal with containment performance obviously need a Level 2 analysis as described in this chapter. A Level 2 analysis is also needed if the application requires that a numerical value for the frequency of a particular release be determined. Finally, if a particular PRA application requires estimates of offsite consequences and integrated risk, as, for example, in the calculation of the U.S. Nuclear Regulatory Commission (NRC) Safety Goal Quantitative Health Objectives (QHOs), then a Level 2 PRA coupled with a Level 3 PRA is needed. Accidents initiated by internal events including internal fires and floods are addressed in the following section. Accidents initiated by various external events are addressed in Chapter 5.

The primary objective of the Level 2 portion of a PRA is to characterize the potential for, and the magnitude and timing of, a release of radioactive material to the environment *given* the occurrence of an accident that results in sufficient damage to the core to cause the release of radioactive material from fuel. To satisfy this objective, a quality Level 2 PRA is comprised of three major parts:

- A quality *Level 1 PRA*, which provides information regarding the accident sequences to be examined and their frequency. The attributes for performing the analyses associated with this aspect of a PRA are described in Chapter 2 and are not discussed further here.
- A structured and comprehensive *evaluation of containment performance* in response to the accident sequences identified from the Level 1 analysis.
- A quantitative *characterization of radiological release* to the environment that would result from accident sequences which breach the containment pressure boundary.

A detailed description of the attributes for conducting the technical analyses associated with each part is provided below.

The current state of knowledge regarding many aspects of severe accident progression and (albeit to a lesser extent) the state of knowledge regarding containment performance limits is imprecise. Therefore, an assessment of containment performance should be performed in a manner that explicitly considers uncertainties in the knowledge of severe accident behavior, the resulting challenges to containment integrity, and the capacity of the containment to withstand various challenges. The potential for a release to the environment is typically expressed in terms of the conditional probability of containment failure (or bypass) for the spectrum of accident sequences (determined from Level 1 PRA analysis) that proceed to core damage.

In addition to estimating the probability of a release to the environment, the Level 2 portion of a PRA should characterize the resulting radiological release to the environment in terms of the magnitude of the core inventory that is released, timing of the release and other attributes important to an assessment of offsite accident consequences. This information provides (1) a quantitative scale with which the relative severity of various accident sequences can be ranked and (2) represents the 'source term' for a quantitative evaluation of offsite consequences (i.e., health effects, property damage, etc.) which are estimated in the Level 3 portion of a PRA.

3 Internal Event Level 2 PRA for Full Power Operations

In the description of the Level 2 PRA below, emphasis is placed on the *level of detail* associated with the major elements of a Level 2 analysis, rather than the specific techniques used to conduct the analysis. This approach is emphasized because several different methods can be used to calculate the probabilistic aspects of severe accident behavior and containment performance. The most common methods are those that use event- and/or fault-tree logic structures; however, other techniques can also be used. Further, the specific methods of quantifying similar logic structures can differ from one study to another. In principle, any of these methods can be considered adequate *provided* it encompasses the level of detail described below.

As indicated above, the two major products of a Level 2 PRA are (1) the conditional probability of containment failure or bypass for accident sequences that proceed to core damage and (2) a characterization of the radiological source term to the environment for each sequence resulting in containment failure or bypass. Although the analyses conducted to generate these products are closely coupled, the characteristics of the analysis to generate them are best described separately. Hence, characteristics of a probabilistic evaluation of containment performance are described in Section 3.1; characteristics of the accompanying estimates of radionuclide release are described in Section 3.2.

3.1 Evaluation of Containment Performance

Although the specific analysis tasks within various Level 2 PRAs may be organized differently, the following three critical elements are included:

- An assessment of the range of challenges to containment integrity (i.e., determination of possible failure mechanisms and range of structural loads);
- Characterization of the capacity of the containment to withstand challenges (i.e., determination of performance limits); and
- A process of organizing and integrating the uncertainties associated with these two evaluations to generate an estimate of the conditional probability that containment would fail (or be bypassed) for a given accident sequence.

Attributes for developing each of these elements are described below.

3.1.1 Assessment of Challenges to Containment Integrity

The primary objective of this element of a Level 2 PRA is to characterize the type and severity of challenges to containment integrity that may arise during postulated severe accidents. An analysis to determine these characteristics acknowledges the dependence of containment response on details of the accident sequence. Therefore, a critical first step is developing a structured process for defining the specific accident conditions to be examined. Attributes for determining which of the many accident sequences generated by Level 1 PRA analysis should be further examined for impact on containment are defined in two parts:

1. Attributes for reducing the large number of accident sequences developed for Level 1 PRA analysis to a practical number for detailed Level 2 analysis; and
2. Attributes for performing and coupling the assessment of containment system performance (i.e., reliability analysis) with Level 1 accident sequence analyses.

3.1.1.1 Defining the Accident Sequences to be Assessed

The primary purpose of Level 1 PRA analysis is to identify the specific combinations of system or component failures (i.e., accident sequence cutsets) that would allow core damage to occur. Unfortunately, the number of cutsets generated by a Level 1 analysis is very large (typically greater than 10,000). It is impractical to evaluate severe accident progression and resulting containment loads for each of these cutsets. As a result, the common practice is to group the Level 1 cutsets into a sufficiently small number of 'Plant Damage States (PDSs)' to allow a practical assessment of the challenges to containment integrity resulting from the full spectrum of accident sequences.

Considerations for the Baseline PRA

Any characteristic of the plant response to a given initiating event that would influence either subsequent containment response or the resulting radionuclide source term to the environment would be represented as an attribute in the PDS binning scheme. These characteristics include:

- *The status of systems that have the capacity to inject water to either the reactor vessel or the containment cavity (or drywell pedestal).* Defining system status simply as "failed" or "operating" is not sufficient in a Level 2 analysis. Low-pressure injection systems may be available but not operating at the onset of core damage because they are 'dead-headed' (i.e., reactor vessel pressure is above their shutoff head). Such states are distinguished from low-pressure injection 'failed' to account for the capability of dead-headed systems to discharge after reactor vessel failure (i.e., providing a mechanism for flooding the reactor cavity).
- *The status of systems that provide heat removal from the reactor vessel or containment.* Careful attention should be paid to the interactions between such systems and coolant injection systems. For example, limitations in the capability for dual-function systems such as the Residual Heat Removal (RHR) system in most boiling water reactors (BWRs) (which provides pumping capacity for low-pressure coolant injection (LPCI) and heat removal for suppression pool cooling) should be properly accounted for.
- *Recoverability of 'failed' systems after the onset of core damage.* Typical recovery actions include restoration of alternating current (AC) power to active components and alignment of non-safety-grade systems to provide (low-pressure) coolant injection to the reactor vessel or to operate containment sprays. Constraints on recoverability (such as no credit for repair of failed hardware) are defined in a manner that is consistent with recovery analysis in the Level 1 PRA.
- *The interdependence of various systems for successful operation.* For example, if successful operation of a LPCI system is necessary to provide adequate suction pressure for successful operation of a high-pressure coolant injection (HPCI) system, failure of the low-pressure system (by any mechanism) automatically renders the high-pressure system unavailable. This information may only be indirectly available in the results of the Level 1 analysis, but should be explicitly represented in the PDS attributes if recovery of the low-pressure system (after the onset of core damage) is modeled.

Several subtle aspects of the mapping of accident sequence cutsets from the Level 1 analysis to the PDSs used as input to a Level 2 analysis should be noted at this point.

- The entire core damage frequency (CDF) generated by the Level 1 analysis is carried forward into the definition of the PDSs which are the entry points to the Level 2 analysis. A minimum ('cut-off') frequency

3 Internal Event Level 2 PRA for Full Power Operations

is not defined as a means of screening out less-important accident sequences. The objective is to allow the risk contribution from low-frequency/high-consequence accident sequences to be captured.

- The mapping from the Level 1 analysis to the PDSs is performed at the cutset level, not the accident sequence level.
- For some accident sequences, the status of all systems may not be determined from the sequence cutsets. For example, if the success criteria for a large break loss-of-coolant accident (LOCA) in a pressurized water reactor (PWR) require successful accumulator operation, the large LOCA sequence cutsets involving failure of all accumulators will contain no information about the status of other coolant injection systems. Realistic resolution of the status of such systems, however, often provides a mechanism for representing accident sequences that are arrested before substantial core damage and radionuclide release occurs. In a Level 2 analysis, these systems are not simply assumed to operate as designed. Their failure frequencies are estimated in a manner that preserves relevant support system dependencies. These are then numerically combined with the sequence cutset frequencies from the Level 1 analysis.

Application Impact Considerations

It is possible that a particular change to a plant's current licensing basis (CLB) may affect the way in which accident sequences are binned into PDSs. For instance, if the proposed change involves the operability of a particular containment system, this could influence the manner in which the system is accounted for in the PDS attributes.

Interfaces with Other Tasks

This task provides the interface between the accident sequences identified by the CDF analysis and the subsequent accident progression analysis. The large number of cutsets generated by the Level 1 analysis is reduced to a practical number of PDSs which serve as the starting point for the Level 2 analysis. This task is a crucial step in assuring that the accident sequences are correctly characterized in terms of containment performance and radionuclide release.

Documentation

In general, sufficient information should be provided in the documentation to allow an independent analyst to reproduce the results. At a minimum, the following should be provided:

- a thorough description of the procedure used to group (bin) individual accident cutsets into PDSs, or other reduced set of accident scenarios for detailed Level 2 analysis;
- a listing of the specific attributes or rules used to group cutsets; and
- a listing and/or computerized database providing cross reference for cutsets to PDSs and vice versa.

3.1.1.2 Assessment of Containment System Performance

The reliability of systems whose primary function is to maintain containment integrity during accident conditions are not always completely incorporated in the accident sequence analysis performed by Level 1 PRA. Such systems may include containment isolation, fan coolers, distributed containment sprays, and hydrogen igniters. Neglecting these

systems (or a simplified representation of them) in Level 1 analyses is common practice because their operation may not play any role in preventing core damage following a postulated accident initiating event. An assessment of the reliability of these systems is, therefore, incorporated in a Level 2 analysis to ascertain whether they would operate as designed to provide containment response during core damage accidents.

Considerations for the Baseline PRA

The methods, scope and technical rigor used to evaluate the reliability of the containment isolation/heat removal systems are comparable to that used in the Level 1 analysis of other 'frontline' systems (refer to Chapter 2). Fault tree models (or other techniques) for estimating failure probabilities are developed and linked directly to the accident sequence models from the Level 1 PRA. This linkage is necessary to properly capture the important influence of mutual dependencies between failure mechanisms for containment systems and other systems. Obvious examples include support system dependencies, such as electrical power, component cooling water, and instrument/control air. Other dependencies that need to be represented in a manner consistent with the Level 1 system models, however, are more subtle. For example,

- Indirect failure of containment safety systems due to harsh environmental conditions (resulting from failure of a support system) should be represented in the assessment of containment system reliability. One important example is failure of reactor or auxiliary building room cooling causing the failure of containment systems due to high ambient temperatures.
- The impact of containment system operation prior to the onset of core damage should be accounted for in the evaluation of system operability after the onset of core damage.
- The human reliability analysis associated with manual actuation of containment systems (e.g., hydrogen igniters) should take into account operator performance during earlier stages of an accident sequence. This analysis should follow the same practices used in the Level 1 analysis as described in Chapter 2.

The long-term performance of containment systems should also be evaluated although the issues to be considered may differ substantially from those listed above. Degradation of the environment within which systems are required to operate as an accident sequence proceeds in time should be taken into account.

In all cases, the assessment of failure probability for containment systems should be based on realistic performance limits rather than bounding (design basis or equipment qualification) criteria.

Application Impact Considerations

As noted in the Introduction, the containment systems may be incorporated into the PRA model in a rather simplified fashion. It is possible that a particular change to a plant's CLB may affect the way a containment system performs or is operated. The modeling of this system should, therefore, be at a level of detail which can reflect this change in performance or operation.

Interfaces with Other Tasks

The results from this task provide some of the information necessary for the quantification of the containment event trees. This task also interfaces with the system performance evaluations performed for the Level 1 analysis.

3 Internal Event Level 2 PRA for Full Power Operations

Documentation

Documentation of containment system performance assessments should include a description of information used to develop containment systems' analysis models and link them with other system reliability models. This documentation should be prepared in the same manner as that generated in the Level 1 analysis of other systems (previously discussed Chapter 2).

3.1.1.3 Evaluation of Severe Accident Progression

Accident analysis codes [such as the Modular Accident Analysis Program (MAAP) (Ref. 3.1) or MELCOR (Ref. 3.2)] provide a framework within which the evolution of events in a severe accident can be accounted for in an integrated fashion. Consequently, the results of these calculations typically provide a basis for estimating the timing of major accident events and for characterizing a range of potential containment loads.

Although code calculations are a useful part of an evaluation of severe accident progression, their results do not form the sole basis for characterizing challenges to containment integrity in a quality Level 2 PRA. There are several reasons for this:

- Many of the models embodied in severe accident analysis codes address highly uncertain phenomena. In each case, certain assumptions are made (either by the model developers or the code user) regarding controlling physical processes and the appropriate formulation of models that represent them. In some instances, the importance of these assumptions can be tested via parametric analysis. However, the extent to which the results of any code calculation can be demonstrated to be robust in light of the numerous uncertainties involved is severely limited by practical constraints of time and resources. Therefore, the assumptions inherent in many code models remain untested.
- None of the integral severe accident codes contain models to represent all accident phenomena of interest. For example, models for certain hydrodynamic phenomena such as buoyant plumes, intra-volume natural circulation, and gas-phase stratification, are not represented in most integral computer codes. Similarly, certain severe accident phenomena, such as dynamic fuel-coolant interactions (i.e., steam explosions) and hydrogen detonations, are not represented.
- It is simply impractical to perform an integral calculation for all severe accident sequences of interest.

As a result, the process of evaluating severe accident progression involves a strategic blend of plant-specific code calculations, applications of analyses performed in other prior PRAs or severe accident studies, focused engineering analyses of particular issues, and experimental data. The manner in which each of these sources of information are used in a Level 2 PRA is described below.

Considerations for the Baseline PRA

The following are used to determine the number of plant-specific calculations that would be performed using an integral code to support a Level 2 PRA:

- At least one integral calculation (addressing the complete time domain of severe accident progression) is performed for each plant damage state. However, this may not be practical depending on the number of plant

damage states developed according to the above discussion. As a minimum, calculations are performed to address the dominant accident sequences (i.e., those with the highest contribution to the total core damage frequency). Calculations are also performed to address sequences that are anticipated to result in relatively high radiological releases (e.g., containment bypass scenarios).

In addition to the calculations of a spectrum of accident sequences described above, several sensitivity calculations are performed to examine the effects of major uncertainties on calculated accident behavior. For example, multiple calculations of a single sequence are performed in which code input parameters are changed to investigate the effects of alternative assumptions regarding the timing of stochastic events (such as operator actions to restore water injection) or the models used to represent uncertain phenomena (such as the size of the opening in containment following overpressure failure). These calculations provide information that is essential to the quantitative characterization of uncertainty in the Level 2 probabilistic logic models (refer to the discussion of logic model development and assignment of probabilities below).

Table 3.1 lists phenomena that can occur during a core meltdown accident and involve considerable uncertainty. This list was based on information in NUREG-1265 (Ref. 3.3), NUREG/CR-4551 (Ref. 3.4) and other studies. It is recognized that considerable disagreement persists within the technical community regarding the magnitude (and in some cases, the specific source) of uncertainty in several of the phenomena listed in Table 3.1. A major objective of the panels assembled as part of the research program that culminated in NUREG-1150 (Ref. 3.5) was to translate the range of technical opinions within the severe accident research community into a quantitative measure of uncertainty on specific technical issues. In a Level 2 PRA, the results of this effort are used as guidance for defining the range of values of uncertain modeling parameters to be used in the sensitivity calculations described above.

Table 3.1 Severe accident phenomena

| Phenomena | Characteristics of accident phenomena |
|---|--|
| Hydrogen generation and combustion | <ul style="list-style-type: none"> Enhanced steam generation from melt debris relocation Steam starvation caused by degraded fuel assembly flow blockage Clad ballooning Recovery of coolant injection systems Steam hydrogen distribution within containment De-inerting due to steam condensation or spray operation |
| Induced failure of the reactor coolant system pressure boundary | <ul style="list-style-type: none"> Natural circulation flow patterns within the reactor vessel upper plenum, hot legs, and steam generators Creep rupture of hot leg nozzles, pressurizer surge line, and steam generator U-tubes |
| Debris bed coolability and core-concrete interactions | <ul style="list-style-type: none"> Debris spreading depth on the containment floor Crust formation at debris bed surface and effects on heat transfer Debris fragmentation and cooling upon contact with water pools Steam generation and debris oxidation |
| Fuel-coolant interactions | <ul style="list-style-type: none"> Potential for dynamic loads to bounding structures Hydrogen generation during melt-coolant interaction |

Table 3.1 Severe accident phenomena

| Phenomena | Characteristics of accident phenomena |
|---|---|
| Melt debris ejection following reactor vessel failure | <ul style="list-style-type: none"> • Melt debris state and composition in the lower head • Mode of lower head failure • Debris dispersal and heat transfer following high-pressure melt ejection |
| Shell melt-through failure in Mark I containments | <ul style="list-style-type: none"> • Melt spreading dynamics • Effects of water • Shell heat transfer and failure mechanism |

A fundamental design objective of the integral severe accident analysis codes used to support a Level 2 PRA (e.g., MAAP, MELCOR) is that they be fast running. Efficient code operation is necessary to allow sensitivity calculations to be performed within a reasonably short time and with minimal resources. One consequence of this objective, however, is that many complex phenomena are modeled in a relatively simple manner or, in some cases, are not represented at all. Therefore, a Level 2 PRA addresses the inherent limitations of integral code calculations in two respects. First, the importance of phenomena not represented by the integral codes are evaluated by some other means (i.e., either application of specialized computational models or by comparison with experimental investigations). Secondly, the effects of modeling simplifications are examined by comparisons with mechanistic code calculations.

In summary, evaluating severe accident progression involves a complex process of plant-specific sensitivity studies using integral codes, mechanistic code calculations, use of prior calculations, experimental data and expert judgement. Examples of this process are given for each of the phenomena in Table 3.1 in the following sections.

Hydrogen Generation and Combustion

Hydrogen phenomena was identified in the NUREG-1150 study as an area where considerable uncertainty existed and, hence, issues associated with hydrogen phenomena were addressed by NUREG-1150 panels. Since these expert panels explicitly considered the uncertainties associated with key phenomena and accounting for uncertainties in the initial and boundary conditions, developed distributions that characterized these uncertainties, the information from these panels provides a convenient and important framework for assessing uncertainties for this application.

The uncertainty in the amount of hydrogen produced during the in-vessel phase of a severe core damage accident was addressed in the NUREG-1150 study by the In-Vessel Panel. Results from this panel are provided in NUREG/CR-4551, Volume 2, Part 1, for both PWRs and BWRs. In that report, distributions are provided for the percentage of in-vessel zirconium that is oxidized.

Clearly, as evident by the NUREG-1150 distributions, there is considerable uncertainty in the amount of zirconium oxidized in vessel and the use of a single number (for example from a MELCOR or MAAP code calculation) is not adequate. While these codes can all predict the amount of hydrogen produced during an accident, the amounts that they predict often vary since they model the phenomena differently. Similarly, a series of sensitivity evaluations with a single code is usually not sufficient to assess the uncertainties since typically a single code will not include all of the

relevant phenomena. Instead, a PRA should include distributions such as those developed by the In-Vessel Panel to characterize the uncertainty in the amount of hydrogen generated during the in-vessel phase of the accident.

Uncertainties in the impact of hydrogen combustion phenomena on the containment were addressed in the NUREG-1150 study by the Containment Loads Expert Panel. For PWRs, hydrogen combustion is a more significant concern in the smaller volume ice condenser containments than it is in the large volume containments. For BWRs, hydrogen combustion is typically only a concern for plants with Mark III containments since both the Mark I and Mark II containments are inerted during normal operation and past PRAs have considered this method reliable under most accident conditions. Hence, the Containment Loads Panel assessed the combustion phenomena at the Grand Gulf plant (BWR, Mark III) and the Sequoyah plant (PWR, Ice Condenser). Information regarding the incorporation of this information into the NUREG-1150 PRAs are provided in NUREG/CR-4551, Volume 5 (Ref. 3.6) for the Sequoyah plant analysis and in NUREG/CR-4551, Vol. 6 (Ref. 3.7) for the Grand Gulf plant analysis.

Since information relevant to hydrogen combustion tends to be specific to the plant and the accident sequences being analyzed, relevant deterministic calculations are used to provide guidance when determining the amount of steam in the containment atmosphere and for determining the distribution of gases in the various compartments. Considering these characteristics, the concentrations of hydrogen, oxygen, and steam are determined for each containment volume where combustion is a concern. These concentrations are then used to determine whether a combustible mixture exists. Of particular concern are local areas where hydrogen can accumulate and thereby form a mixture that can potentially detonate. For compartmentalized containments, such as ice condenser containments, there can be considerable uncertainty in these concentrations for the various compartments necessitating the development of uncertainty distributions. A discussion of these uncertainties for an ice condenser containment can be found in Section 5.2 of NUREG/CR-4551, Vol. 2, Part 2, Rev. 1. The calculation of the total concentration of hydrogen in containment takes into account both the hydrogen produced in vessel and ex vessel (through the core-concrete interaction) in cases where the containment does not fail at vessel breach.

Combustible mixtures that form in the containment can be ignited from a number of sources including igniters, AC powered equipment, and hot surfaces. For situations where there are no identifiable ignition sources, such as during a station blackout, it is still possible for a combustible mixture of hydrogen to ignite since ignition requires very little energy. The ignition of hydrogen under this last condition was addressed in NUREG-1150 by the Containment Loads Panel. Results from this panel are provided in Section 5.1 for the Grand Gulf plant (BWR, Mark III) and Section 5.2 for the Sequoyah plant (PWR, Ice Condenser) NUREG/CR-4551, Vol. 2, Part 2. The panel provided distributions that characterized the uncertainty in the ignition frequency for situations where AC power is not available in the containment.

Quasi-static loads from hydrogen combustion events were assessed in the NUREG-1150 study by the Containment Loads panel for both the Grand Gulf and the Sequoyah plants. Generally, the experts based the peak overpressures on the adiabatic isochoric complete combustion model and then corrected the pressures to account for burn completeness, heat transfer and expansion into non-participating compartments. For the PWR plant, the experts felt that the uncertainty in the peak overpressure was small compared to the uncertainties in the hydrogen concentration

¹Here combustion refers to combustion in the containment. However, following failure of the containment, combustion of hydrogen in the reactor buildings surrounding Mark I and Mark II containments can also be a concern. Combustion in the reactor building surrounding a Mark I plant was addressed by the Containment Loads Expert Panel and is discussed in Section 5.3 of NUREG/CR-4551, Vol. 2, Rev. 1, Part 2.

3 Internal Event Level 2 PRA for Full Power Operations

and ignition frequencies and hence a single estimate of the peak overpressure as a function of hydrogen concentration was provided instead of a probability distribution. These estimates are provided in Section 5.2 in NUREG/CR-4551, Vol. 2, Part 2, Rev. 1. For the BWR plant the uncertainty in the peak overpressure was driven by the uncertainty in the burn completeness (although it was also acknowledged by these experts that the uncertainty in the ignition frequency is a key uncertainty associated with the hydrogen combustion phenomena) and, hence probability distributions were developed. The distributions developed by this panel are provided in Section 5.1 of NUREG/CR-4551, Volume 2, Part 2.

Since the publication of NUREG-1150, some additional research has been conducted on combustion of hydrogen-air-steam mixtures in condensing environments (Ref. 3.8). In these experiments, ignition was provided by thermal igniters. These experimental results provide relevant information that was not available during the NUREG-1150 study and may be referenced when assessing the peak pressure in a rapidly condensing environment with igniters available.

Hydrogen detonations in the Grand Gulf and Sequoyah containments were also addressed by the Containment Loads Panel and are discussed in Sections 5.1 and 5.2 of NUREG/CR-4551, Vol. 2, Part 2, Rev. 1, respectively. The panel assessed the frequency of a deflagration to detonation transition (DDT). The DDT frequency was analyzed considering different locations within the containment and different concentrations of hydrogen within each location. The probability distributions that characterize the uncertainty in the DDT frequency are broad for both the BWR and the PWR plants. Given that a detonation occurs, the expert panel also assessed the resulting peak impulse. The geometry in the area where the ignition occurs is a key uncertainty that affects the likelihood that a DDT will occur. Similarly, the interaction between the detonation wave and structures is a key uncertainty that affects the peak impulse.

Induced Failure of the Reactor Coolant System (RCS) Pressure Boundary

The possibility of a temperature-induced rupture of the steam generator (SG) tubes is affected by several factors including the thermal hydraulic conditions at various locations in the primary system, which determine the temperatures (and the time at those temperatures) and the pressures to which the SG tubes are subjected as the accident progresses. Other relevant factors include the effective temperature required for creep rupture failure of the SG tube, and the presence of pre-existing defects in the SG tubes which increase the likelihood of rupture.

In NUREG-1150, this issue was treated in the expert elicitation process. All experts agreed that hot leg failure, including failure of the surge line, was much more likely to occur before a rupture of a steam generator tube. Two experts felt that pre-existing defects in the SG tubes could lead to a higher probability of SG tube rupture (SGTR). The third expert felt that due to the long time lag between temperatures in the hot leg and the SG tubes, the frequency of temperature-induced SGTR was so small that it could be expressed as a (small) constant value regardless of pre-existing defects.

A conditional probability distribution of temperature-induced SGTR was developed in NUREG-1150 by aggregating the individual distributions provided by three experts. A discussion of the phenomenon and the assignment of the conditional probability distribution of temperature-induced SGTR is contained in NUREG/CR-4551, Vol. 2. This distribution was applied in the accident progression event trees developed for the Zion and for the Surry plants in NUREG-1150. The Zion and Surry reports [NUREG/CR-4551, Vol. 7 (Ref. 3.9) and NUREG/CR-4551, Vol. 3 (Ref. 3.10) respectively] can be consulted for information related to how the conditional probability distribution of temperature-induced SGTR should be applied to obtain the split fractions for the containment event tree for this issue.

Debris Bed Coolability and Core-Concrete Interactions (CCI)

Debris coolability is an important issue because if the debris is brought to a coolable geometry, the only source for containment pressurization will be the generation of steam from boiloff of the overlying water. This is a slow process and, in the absence of containment heat removal, would result in very late containment failure allowing ample time for remedial actions. Furthermore, a coolable debris geometry would limit basemat penetration.

In addition, if a coolable debris bed is formed in the cavity or pedestal and makeup water is continuously supplied then interactions between the core debris and concrete will be minimized and release of radioactive material from this source would be avoided.

If CCI does occur (i.e., the debris bed is not coolable), experimental results indicate that the presence or absence of an overlying water pool does not have much effect on the downward progression of the melt front.

The mechanisms that govern debris coolability are conduction heat transfer, shrinkage cracking, gas sparging and melt eruption, and crust failure under the weight of the water. Experimental research (Ref. 3.11) has been carried out to investigate this issue. These tests include the SWISS-1 (Ref. 3.12) and -2, FRAG-3 and -4, (Ref. 3.13) WETCOR-1, (Ref. 3.14) and MACE (Ref. 3.15) series of tests. This experimental information would be considered in a quality PRA when developing distributions for the likelihood of forming a coolable debris bed for a particular plant configuration. The expert panel convened for NUREG-1150 specifically for molten-core-concrete interaction issues is an example of how major input parameters for this issue are quantified.

Fuel-Coolant Interactions

For an accident leading to a severely damaged core, the probability of an in-vessel steam explosion causing early containment failure was assumed in WASH-1400 to be between 0.1 and 0.01. In 1985, the first Steam Explosion Review Group (SERG-1) workshop was held to systematically evaluate the alpha-mode failure issue. The experts who participated in that workshop reviewed the then current understanding of the potential for containment failure from in-vessel steam explosion. They reached a nearly unanimous opinion that the probability of alpha-mode failure is less than that used in WASH-1400. NRC-sponsored research carried out since 1985 has played a major role in developing an understanding of the key physical processes involved in energetic fuel coolant interactions (FCIs).

In June 1995, the second SERG (SERG-2) workshop was held to revisit the alpha-mode failure issue, and to evaluate the current understanding of other FCI issues that could potentially contribute to risk, such as shock loading of the lower head and ex-vessel support structures. The estimates of failure probability expressed by SERG-2 experts were generally an order of magnitude lower than the SERG-1 estimates.

Melt Debris Ejection Following Reactor Vessel Failure

In certain severe accidents, the failure of the reactor pressure vessel (RPV) can occur while the RCS is at elevated pressure. In these accidents, the expulsion of the molten core debris and blow down of the RCS could lead to a very rapid and efficient heat transfer to the containment atmosphere, possibly accompanied by oxidation reactions and hydrogen combustion that further enhances the energy transfer. These processes, which lead to containment pressurization, are collectively referred to as direct containment heating (DCH). Overpressurization resulting from DCH is a significant containment challenge that can lead to early containment failure.

3 Internal Event Level 2 PRA for Full Power Operations

The results of a probabilistic assessment of DCH-induced containment failure for the Zion Nuclear Power Plant were published in NUREG/CR-6075 (Ref. 3.16) and its supplement, NUREG/CR-6338 (Ref. 3.17) used the methodology and scenarios described in NUREG/CR-6075 to address the DCH issue for all Westinghouse plants with large volume containments, including 34 plants with large dry containments and seven plants with subatmospheric containments. DCH loads versus strength evaluation were performed in a consistent manner for all plants. The phenomenological modeling was closely tied to the experimental database. Plant-specific analyses were performed, but sequence uncertainties were enveloped by a small number of splinter scenarios without assignment of probabilities. The results of screening calculations reported in NUREG/CR-6338 indicate that only one plant showed a conditional containment failure probability (CCFP) based on the mean fragility curves greater than 0.001. The CCFP for this one plant was found to be less than 0.01. These results can, therefore, be used for Level 2 PRAs for Westinghouse plants with large volume containments. For BWRs and other PWR plants, the methodology reported in NUREG/CR-6338 for performing load/strength evaluations using the plant-specific input to the two-cell equilibrium model or appropriate containment analysis codes, can be used to provide a PRA-integrated perspective on this issue. For plants with ice condenser containments, it is believed that the ice chamber in the plant can, to a certain extent, trap dispersing core debris, and provide cooling to moderate the effect of DCH.

Shell Melt-through Failure in Mark I Containments

To address the shell melt issue in NUREG-1150, a panel of experts was convened to provide input as to the probability of shell melt for five scenarios: (1) low and medium flow with water, (2) low and medium flow without water, (3) high flow with water, (4) high flow without water and two of three parameters (pressure, fraction of metal, and superheat) high, and (5) high flow without water and two of three parameters (pressure, fraction of metal, and superheat) low. The individual elicitations were then averaged and presented in Table 6-1 of NUREG/CR-4551, Volume 2, Part 2.

In a more recent report, Theofanous et al. published a probabilistic methodology in NUREG/CR-6025 (Ref. 3.18) as an overall systematic approach for addressing the Mark I shell melt-through issue.

The above approaches are examples of generating probabilistic information on shell melt-through. A Level 2 PRA would investigate plant-specific design features, including pedestal door arrangement (and relative alignment of downcomers), drywell floor area and sump volumes, and in particular, the amount of fuel in the reactor and the downcomer entrance height above the drywell floor. The downcomer entrance height affects not only the amount of water attainable on the floor, but more importantly, if the amount of fuel is sufficient that melt can run directly into the downcomer, liner failure is virtually assured. The probabilities of shell melt-through should apply to a steel lined reinforced concrete containment, however, if sufficient technical basis is provided, the effective failure size in the containment structure may be adjusted accordingly (though there should be no credit given for "self-healing" of the containment boundary).

Application Impact Considerations

A change in a plant's CIB can affect the way a plant system performs or operates. If the plant system(s) in question could have an influence on the accident progression, then the accident progression analysis should account for the change in the systems' performance or operation. For example, a degraded power supply to hydrogen igniters could influence the likelihood and severity of a hydrogen combustion event in the containment, or the removal of a backup water supply could reduce the chances for achieving debris bed coagulability and increase the possibility of core-concrete interaction. An operational example would be a change in procedures related to the restart of the reactor coolant

pumps under degraded core conditions which could influence the likelihood of an induced failure of the RCS pressure boundary.

Interfaces with Other Tasks

This task provides the bulk of the information for quantifying the containment event trees. The conditions produced by the various severe accident phenomena should also be considered for the assessment of the performance of containment systems.

Documentation

Documentation of analyses of severe accident progression should include the following:

- a description of plant-specific accident simulation models (e.g., MAAP or MELCOR) including extensive references to source documentation for input data.
- a listing of all computer code calculations performed and used as a basis for quantifying any event in the containment probabilistic logic model including a unique calculation identifier or name, a description of key modeling assumptions or input data used, and a reference to documentation of calculated results. (If input and/or output data are archived for quality assurance records or other purposes, an appropriate reference to calculation archive records is also provided.).
- a description of key modeling assumptions selected as the basis for performing "base case" or "best-estimate" calculations of plant response and a description of the technical bases for these assumptions.
- a description of plant-specific calculations performed to examine the effects of alternate modeling approaches or assumptions.
- if analyses of a surrogate (i.e., 'similar') plant are used as a basis for characterizing any aspect of severe accident progression in the plant being analyzed, references to, or copies of documentation of the original analysis, and a description of the technical basis for assuring the applicability of results, and
- for all other original engineering calculations, a sufficiently complete description of the analysis method, assumptions and calculated results is prepared to accommodate an independent (peer) review.

3.1.2 Establishing Containment Performance Limits

The objective of this element of a Level 2 PRA is to determine the loading limits (or capacity) that the containment can withstand given the range and magnitude of the potential challenges. These challenges take many forms, including internal pressure rises (that occur over a sufficiently long time frame that they can be considered "static" in terms of the structural response of the containment), high temperatures, thermo-mechanical erosion of concrete structures, and under some circumstances, localized dynamic loads such as shock waves and internally generated missiles. Realistic estimates for the capacity of the containment structure to withstand these challenges are generated to provide a benchmark against which the likelihood of containment failure can be estimated.

3 Internal Event Level 2 PRA for Full Power Operation is

in a Level 2 PRA, the attributes of the analyses necessary to characterize containment performance limits are consistent with those of the containment load analyses against which they will be compared

- They focus on plant-specific containment performance (i.e., application of reference plant analyses is generally inadequate)
- They consider design details of the containment structure such as:
 - containment type (free-standing steel shell; concrete-backed steel shell; pre-stressed, post-tensioned, or reinforced concrete)
 - the full range of penetration sizes, types, and their distribution (equipment and personnel hatches, piping penetrations, electrical penetration assemblies, ventilation penetrations)
 - penetration seal configuration and materials
 - discontinuities in the containment structure (shape transitions, wall anchorage to floors, changes in steel shell or concrete reinforcement)
- They consider interactions between the containment structure and neighboring structures (the reactor vessel and pedestal, auxiliary building(s), and internal walls)

3.1.2.1 Considerations for the Baseline PRA

A thorough assessment of containment performance generally begins with a structured process of identifying potential containment failure modes (i.e., mechanisms by which integrity might be violated). This assessment commonly begins by reviewing a list of failure modes identified in PRAs for other plants to determine their applicability to the current design. Such a list was incorporated in the NRC's guidance for performing an individual plant examination (IPE) (Ref. 3-19). This review is then supplemented by a systematic examination of plant-specific design features and emergency operating procedures to ascertain whether additional, unique failure modes are conceivable. For each plausible failure mode, containment performance analyses are performed using validated structural response models, as well as plant-specific data for structural materials and their properties.

For many containment designs, overpressure has been found to be a dominant failure mechanism. In a quality Level 2 PRA, the evaluation of ultimate pressure capacity is performed using a plant-specific, finite-element model of the containment pressure boundary including sufficient detail to represent major discontinuities such as those listed above. The influence of time-varying containment atmosphere temperatures is taken into account by performing the calculation for a reasonable range of internal temperatures. To the extent that internal temperatures are anticipated to be elevated for long periods of time (e.g., during the period of aggressive core-concrete interactions), thermal growth and creep rupture of steel containment structures is taken into account.

The characterization of containment performance limits is not simply a matter of defining a threshold load at which the structure "fails." A Level 2 PRA attempts to distinguish between structural damage that results in "catastrophic failure" of the containment from damage that results in significant leakage² to the environment. Leakage is often characterized by a smaller opening (i.e., one that may not preclude subsequent increases in containment pressure).

²Significant leakage is defined relative to the design basis leakage for the plant. Leakage rates greater than 100 times the design basis have been found risk significant in past studies.

Failure to isolate the containment is also considered. It is very important to assess both the location and size of the containment failure because of the implications for the source term calculation, e.g., given the same in-vessel and ex-vessel releases inside containment, a rupture in the drywell of a Mark II containment will result in higher releases to the environment than a leak in the wetwell.

Current models for the response of complex structures to even "simple" loads (such as internal pressure) are not sufficiently robust to allow simultaneous prediction of a failure threshold and resulting failure size. This is particularly true for structures composed of non-homogeneous materials with highly non-linear mechanical properties such as reinforced concrete. As a result, calculations to establish performance limits are supplemented with information from experimental observations of containment failure characteristics and expert judgment. Examples of this process can be found in NUREG-1150.

Failure location and size by dynamic pressure loads and internally generated missiles should also be probabilistically examined. The structural response panel for NUREG-1150 assessed the size and location of the containment breach by dynamic pressure loads for Grand Gulf (reinforced concrete) and Sequoyah (free-standing steel). Both leaks and ruptures were predicted to occur in the containment response to detonations at Grand Gulf, and ruptures were predicted to occur at Sequoyah. Alpha mode failure (for all NUREG-1150 plants) and steel shell melt-through of a containment wall by direct contact of core debris (for Peach Bottom and Sequoyah) were treated as rupture failures of containment in NUREG-1150.

Basemat melt-through is generally treated as a leak in most Level 2 PRAs because of the protracted times involved as well as the predicted radionuclide retention in the soil. If a bypass of containment, such as an interfacing systems LOCA, is predicted to occur, then its effective size and location (e.g., probability that the break is submerged in water) are also estimated in order to perform the source term calculations.

3.1.2.2 Application Impact Considerations

A change in the plant's CLB could impact the limits of containment performance. The containment structural capability or the reliability of containment isolation could be affected by changes in equipment or inspection levels, etc. If this is a consideration, the analysis of the containment performance limits should be detailed enough to account for such an impact. For instance, if a change in the CLB could affect the containment isolation system, this system should be modeled in sufficient detail to reflect this change.

3.1.2.3 Interfaces with Other Tasks

The containment performance limits established by this task form a crucial input to the probabilistic assessment of the containment performance and the ability of the containment to withstand the challenges from severe accidents.

3.1.2.4 Documentation

In general, sufficient information in the documentation of analyses performed to establish quantitative containment performance limits is provided that allows an independent analyst to reproduce the results. At a minimum, the following information is documented for a PRA:

- a general description of the containment structure including illustrative figures to indicate the general configuration, penetration types and location, and major construction materials.

3 Internal Event Level 2 PRA for Full Power Operations

- a description of the modeling approach used to calculate or otherwise define containment failure criteria.
- if computer models are used (e.g., finite element analysis to establish overpressure failure criteria), a description of the way in which the containment structure is nodalized including a specific discussion of how local discontinuities, such as penetrations, are addressed, and
- if experimentally determined failure data are used, a sufficiently detailed description of the experimental conditions to demonstrate applicability of results to plant-specific containment structures.

3.1.3 Probabilistic Modeling of Containment Performance

The way in which uncertainties are represented in the characterization of containment performance³ is an important consideration in a Level 2 PRA. In particular, explicit and quantitative recognition should be given to uncertainties in the individual processes and parameters that influence severe accident behavior and attendant containment performance. These uncertainties are then quantitatively integrated by means of a probabilistic logic structure that allows the conditional probability of containment failure to be quantitatively estimated, as well as the uncertainty in the containment failure probability.

Two elements of such an assessment are described below. First, the characteristics of the logic structure used to organize the various contributors to uncertainty are described. However, the major distinguishing element of an approach to characterizing containment performance is the assignment and propagation of uncertainty distributions for major events in the logic model. The key phrase here is uncertainty distributions (i.e., point estimates of probability are not universally applied to the logic model). Characteristics of these distributions and the manner in which they are used in a typical logic model are described later in this section.

3.1.3.1 Considerations for the Baseline PRA

The primary function of a "containment event tree," or any other probabilistic model evaluating containment performance, is to provide a structured framework for organizing and ranking the alternative accident progressions that may evolve from a given core damage sequence or a plant damage state. In developing this framework, whether it be in the form of an event tree, fault tree or other logic structure, several elements are necessary to allow a comprehensive assessment of containment performance:

- Explicit recognition of the important time phases of severe accident progression. Different phenomena may control the nature and intensity of challenges to containment integrity and the release and transport of radionuclides as an accident proceeds in time. The following time frames are of particular interest to a Level 2 analysis:
 - *After the initiating event, but before the onset of core damage.* This time period establishes important initial conditions for containment response after core damage begins.

³Uncertainties in the estimation of radionuclide source terms are also represented in a Level 2 PRA; however, this topic is discussed in Section 3.2.

- *After the core damage begins, but prior to failure of the reactor vessel lower head.* This period is characterized by core damage and radionuclide release (from fuel) while core material is confined within the reactor vessel.
- *Immediately following reactor vessel failure.* Prior analysis of containment performance suggests that many of the important challenges to containment integrity occur immediately following reactor vessel failure. These challenges may be short-lived, but often occur only as a direct consequence of the release of molten core materials from the reactor vessel immediately following lower head failure.
- *Long-term accident behavior.* Some accident sequences evolve rather slowly and generate relatively benign loads to containment structures early in the accident progression. However, in the absence of some mechanism by which energy generated within the containment can be safely rejected to the environment, these loads may steadily increase to the point of failure in the long term.

When linked end-to-end, these time frames constitute the outline for most probabilistic containment performance models. Within each time frame, uncertainties in the occurrence or intensity of governing phenomena are systematically evaluated.

- Consistency in the treatment of severe accident events from one time frame to another. Many phenomena may occur during several different time frames of a severe accident. However, certain limitations apply to the composite (integral) contribution of some phenomena over the entire accident sequence and these are represented in the formulation of a probabilistic model.

A good example is hydrogen combustion in a PWR containment. Hydrogen generated during core degradation can be released to the containment over several time periods. However, an important contribution to the uncertainty in containment loads generated by a combustion event is the total mass of hydrogen involved in a particular combustion event. One possibility is that hydrogen released to the containment over the entire in-vessel core damage period accumulates without being burned (perhaps) as a result of the absence of a sufficiently strong ignition source. Molten core debris released to the reactor cavity at vessel breach could represent a strong ignition source, which would initiate a large burn (assuming the cavity atmosphere is not steam inert). Because of the mass of hydrogen involved, this combustion event might challenge containment integrity. Another possibility is that while the same total amount of hydrogen is being released to the containment during in-vessel core degradation, a sufficiently strong ignition source exists to cause several small burns to occur prior to vessel breach. In this case, the mass of hydrogen remaining in the containment atmosphere at vessel breach would be very small in comparison to the first case, and the likelihood of a significant challenge to containment integrity at that time should be correspondingly lower. Therefore, the logic for evaluating the probability of containment failure associated with a large combustion event occurring at the time of vessel breach is able to distinguish these two cases and preclude the possibility of a large combustion event if hydrogen was consumed during an earlier time frame.

- Recognition of the interdependencies of phenomena. Most severe accident phenomena and associated events require certain initial or boundary conditions to be relevant. For example, a steam explosion can only occur if molten core debris comes in contact with a pool of water. Therefore, it may not be meaningful to consider ex-vessel steam explosions during accident scenarios in which the drywell floor (BWR) or reactor cavity (PWR) is dry at the time of vessel breach. Logic models for evaluating containment performance capture these and many other such interdependencies among severe accident events and phenomena. Explicit

3 Internal Event Level 2 PRA for Full Power Operations

representation of these interdependencies provides the mechanism for allowing complete traceability between a particular accident sequence (or PDS) and a specific containment failure mode.

There are many approaches to transforming the technical information concerning containment loads and performance limits to an estimate of failure probability, but three approaches appear to dominate the literature. In the first (least rigorous) approach, qualitative terms expressing various degrees of uncertainty are translated into quantitative (point estimate) probabilities. For example, terms such as "likely" or "unlikely" are assigned numerical values (such as 0.9 and 0.1). Superlatives, such as "very" likely or "highly" unlikely, are then used to suggest "degrees of confidence that a particular event outcome is appropriate. The subjectivity associated with this method is controlled to some extent by developing rigorous attributes for the amount and quality of information necessary to justify progressively higher confidence levels (i.e., probabilities approaching 1.0 or 0.0). Nonetheless, this method is not considered an appropriate technique for assigning probabilities to represent the state of knowledge uncertainties⁴ in a PRA. Among its weaknesses, this approach simply produces a point estimate of probability and is not a rigorous technique for developing probability distributions.

The second technique involves a convolution of paired probability density functions. In this technique, probability density functions are developed to represent the distribution of credible values for a parameter of interest (e.g., containment pressure load) and for its corresponding failure criterion (e.g., ultimate pressure capacity). This method is more rigorous than the one described above in the sense that it explicitly represents the uncertainty in each quantity in the probabilistic model. The basis for developing these distributions is the collective set of information generated from plant-specific integral code calculations, corresponding sensitivity calculations, other relevant mechanistic calculations, experimental observations, and expert judgment. The conditional probability of containment failure (for a given accident sequence) is then calculated as the convolution of the two density functions. While this technique provides an explicit treatment of uncertainty at intermediate stages of the analysis, it still ultimately generates a point estimate for the probability of containment failure caused by a particular mechanism. The contributions to (and magnitude of) uncertainty in the final (total) containment failure probability is discarded in the process.

The third technique involves adding an additional feature to the technique described above. That is, the probability density functions representing uncertainty in each term of the containment performance logic model are propagated throughout the entire model to allow calculation of statistical attributes such as importance measures. One means for accomplishing this objective is the application of Monte Carlo sampling techniques (such as Latin Hypercube sampling). The application of this technique to Level 2 PRA logic models, pioneered in NUREG-1150, accommodates a large number of uncertain variables. Other techniques have been developed for specialized applications, such as the direct propagation of uncertainty technique developed to assess the probability of containment failure as a result of direct containment heating in a large dry PWR (Ref. 3.16). However, these other techniques are constrained to a small number of variables and are not currently capable of applications involving the potentially large number of uncertain variables addressed in a quality Level 2 PRA.

3.1.3.2 Application Impact Considerations

A change in a plant's CLB could affect the likelihood with which certain containment failures occur and the uncertainties associated with these failures. If this is the case, the probabilistic containment model should be detailed enough to account for the effects of such changes.

⁴Such uncertainties tend to dominate a Level 2 PRA, rather than uncertainty associated with random behavior.

3.1.3.3 Interfaces with Other Tasks

This task integrates many of the results produced from the other tasks discussed. For instance, the containment performance limits established under the previous task provide many of the anchor points for the probability distributions used in this task.

3.1.3.4 Documentation

The following documentation is generated to provide the results and describe the process by which the conditional probability of containment failure is calculated:

- tabulated conditional probabilities of various containment failure modes with specific characterizations of time phases of severe accident progressions (e.g., early vs. late containment failures).
- a listing and description of the structure of the overall logic model used to assemble the probabilistic representation of containment performance (graphical displays of events trees, fault trees or other logic formats are provided to illustrate the logic hierarchy and event dependencies).
- a description of the technical basis (with complete references to documentation of original engineering analyses) for the assignment of all probabilities or probability distributions with the logic structure.
- a description of the rationale used to assign probability values to phenomena or events involving subjective, expert judgment, and
- a description of the computer program used to exercise the logic model and calculate final results

3.2 Radionuclide Release Characterization

The second, albeit equally important, product of a Level 2 PRA is a quantitative characterization of radiological release to the environment resulting from each accident sequence that contributes to the total CDF. In many Level 2 analyses, this information is used solely on a semi-quantitative scale to rank the relative severity of accident sequences. In such circumstances, a rigorous quantitative evaluation of radionuclide release, transport, and deposition may not be necessary. Rather, order-of-magnitude estimates of the release for a few important radionuclide species provide a satisfactory scale for ranking accident severity. In a Level 2 PRA, however, the characterization of radionuclide release to the environment provides sufficient information to completely define the "source term" for use in a Level 3 PRA to calculate offsite consequences. Further, the level of rigor required of the evaluation of radionuclide release, transport, and deposition directly parallels that used to evaluate containment performance. That is,

- Source term analyses (deterministic computer code calculations) reflect plant-specific features of system design and operation. In particular, plant-specific characteristics, such as quantity of fuel, control rod material, and in-core support structure composition and spatial distribution; configuration and deposition areas of primary coolant system and containment structures; reactor cavity (or drywell floor) configuration and concrete composition; and the topology of transport pathways from the fuel and/or core debris to the environment are faithfully represented in the models used to calculate radionuclide source terms.

3 Internal Event Level 2 PRA for Full Power Operations

- Calculations of radionuclide release, transport, and deposition represent sequence-specific variations in primary coolant system and containment characteristics. For example, reactor vessel pressure during in-vessel core melt progression and the operation (or failure) of containment mitigation systems such as distributed sprays are represented in a manner that allows for their effects on radionuclide release and/or transport to be directly accounted for. Radionuclide release calculations also need to take into account scrubbing of the release by passive systems, such as overlying pools of water in the reactor cavity or the suppression pool in BWRs.
- Uncertainties in the processes governing radionuclide release, transport and deposition are quantified. In the same way uncertainties in the phenomena governing severe accident progression are quantified to characterize uncertainty in the probability of containment failure (described above), uncertainties related to radionuclide behavior under severe accident conditions are quantified to characterize uncertainty in the radionuclide source term associated with individual accident sequences.

The specific manner in which radionuclide source terms are characterized in a Level 2 analysis is described first. Attributes for coupling the evaluation of radionuclide release to analyses of severe accident progression for particular sequences are also described. Finally, attributes for addressing uncertainties in radionuclide source terms are described.

3.2.1 Definition of Radionuclide Source Terms

3.2.1.1 Considerations for the Baseline PRA

The analysis of offsite consequences resulting from an accidental release of radionuclides performed in a Level 3 PRA requires specification of several parameters from a Level 2 PRA which define the environmental source term. Ideally, the following information is developed:

- the time at which a release begins.
- the time history of the release of all important radioisotopes that contribute to health effects.
- the chemical form of the isotopes.
- the elevation (above local ground level) at which the release occurs.
- the energy with which the release is discharged to the environment, and
- the size distribution of radioactive material released in the form of an aerosol (i.e., particulate).

As in many other aspects of a comprehensive PRA, it is impractical to generate this information for the full spectrum of accident conditions produced by Level 1 and 2 analyses. To address this constraint, several simplifications are made in a Level 2 analysis. The most significant of these are outlined below.

The following assumptions are typically made in a Level 2 analysis regarding the radioactive material of interest.

- All isotopes of a single chemical element are released from the fuel at the same rate.

- Chemical elements exhibiting similar properties in terms of their measured rate of release from fuel, physical transport through the reactor coolant system and the containment and chemical behavior in terms of interactions with other elemental species and structural surfaces can be effectively modeled as one composite radionuclide specie. Typically, the specific properties of a single (mass dominant) element are used to represent the properties of all species within a group.

Although the radionuclide species are released from fuel in their elemental form, many species quickly combine with other elements to form compounds as they migrate away from their point of release. The formation of these compounds and the associated change in the physico-chemical properties of individual radionuclide groups are taken into account in the analysis of radionuclide transport and deposition. In particular, volatile radionuclide species, such as iodine and cesium, may be transported in more than one chemical form--each with different properties that affect their transport.

Another simplification in the characterization of radionuclide release involves the treatment of time-dependence of the release. In a Level 2 PRA, these variations are reduced to a series of discrete periods of radiological release, each of which is described by a starting time, a duration, and a (constant) release rate. The release rate may be simplified to represent major characteristics of the release history such as an early, short-lived, large release immediately following containment failure followed by a longer period(s) of a sustained release. The specific characteristics of these discrete release periods may vary from one accident sequence (or plant damage state) to another, but the timing characteristics (i.e., start time and duration) should be the same for each radionuclide group (i.e., only the release rate varies from one group to another for a given release period). The total number of release periods is typically small (i.e., 3 or 4) and represent distinct periods of severe accident progression. For example, the following time periods are representative of an accident leading to early structural failure of containment:

- Very early (containment leakage prior to containment failure)
- Puff release (immediately following containment failure)
- Early (relatively large release rate period during aggressive corium-concrete interactions).
- Late (long-term, low release rate following corium-concrete interactions).

Note that the above time periods are for illustrative purposes only; others are developed, as necessary, to suit the specific results of a plant-specific assessment.

3.2.1.2 Application Impact Considerations

The impact of any suggested changes on availability of systems that mitigate radionuclide releases should be assessed.

3.2.1.3 Interfaces with Other Tasks

The radionuclide groupings and release periods chosen will provide the basis for the remaining radionuclide source term tasks.

3.2.1.4 Documentation

Documentation of analyses performed to characterize radiological source terms should provide sufficient information to allow an independent analyst to reproduce the results. At a minimum, the following information should be documented in a PRA:

3 Internal Event Level 2 PRA for Full Power Operation

- The radionuclide grouping scheme used and the assumptions made to obtain it should be clearly described.
- The time periods considered for the release and the rationale for the choices made.

3.2.2 Coupling Source Term and Severe Accident Progression Analyses

The number of unique severe accident sequences represented in a Level 2 PRA can be exceedingly large. Comprehensive, probabilistic consideration of the numerous uncertainties in severe accident progression can easily propagate one accident sequence (or plant damage state) from the Level 1 systems analysis into 10^4 to 10^5 alternative severe accident progressions. A radionuclide source term should be estimated for each of these accident progressions. Clearly, it is impractical to perform that many deterministic source term calculations.

3.2.2.1 Considerations for the Baseline PRA

A common practice in many Level 2 PRAs (although insufficient for a comprehensive assessment) is to reduce the analysis burden by grouping the alternative severe accident progressions into 'source term bins' or 'release categories.' This grouping process is analogous to the one used at the interface between the Level 1 and Level 2 analysis to group accident sequence cutsets into plant damage states. The principal objective of the source term grouping (or binning) exercise is to reduce the number of specific severe accident scenarios, for which deterministic source term calculations should be performed, to a practical value. A structured process similar to the one described in Chapter 2 (related to the assessment of accident sequences addressed in a quality Level 2 PRA) is typically followed to perform the grouping. Characteristics of severe accident behavior and containment performance that have a controlling influence on the magnitude and timing of radionuclide release to the environment are used to bin (or group) the alternative accident progressions into appropriate release categories. A deterministic source term calculation is then performed for a single (typically the highest frequency) accident progression within each release category to represent the entire group.

As indicated above, this approach is inadequate for a Level 2 analysis because the radionuclide source term for any given severe accident progression cannot be calculated with certainty. The influence of uncertainties related to the myriad processes governing radionuclide release from fuel, transport through the primary coolant system and containment, and deposition on intervening structures, is significant and should be quantified with a similar level of rigor afforded to severe accident progression uncertainties. Examples of these uncertainties were given in Chapter 2. Further, a Level 2 PRA is performed in a manner that allows the relative contribution of individual parameter uncertainties to the overall uncertainty in risk to be calculated directly (i.e., via rank regression or some other statistically acceptable manner). This requires a probabilistic modeling process that combines the uncertainty distributions associated with the evaluation of accident frequency, severe accident progression, containment performance, and radionuclide source terms in an integrated, self-consistent fashion.

In performing this integrated uncertainty analysis, special care should be taken to ensure consistency between uncertain parameters associated with radionuclide release, transport and deposition, and other aspects of accident behavior. In particular, important correlations between the behavior of radionuclides and the other characteristics of severe accident progression should be accounted for. These correlations and other similar relationships are described in NUREG/CR-4551 (Ref. 3.20).

3.2.2.2 Application Impact Considerations

If the complete integrated uncertainty approach associated with a Level 2 analysis is performed, it is not likely that changes in a plant's CLB will impact the coupling of the source term and the accident progression analysis.

If a grouping or binning process is chosen and only deterministic source term calculations are performed for specific accident scenarios, then care should be taken that the chosen accident scenarios are capable of reflecting any impact a change in the plant's CLB may have on the source terms.

3.2.2.3 Interfaces with Other Tasks

As noted in the description above, this task requires the integration of the distributions obtained from the evaluation of accident frequency, accident progression, containment performance, and radionuclide source terms.

3.2.2.4 Documentation

Documentation of analyses performed to characterize radiological source terms should provide sufficient information to allow an independent analyst to reproduce the results. At a minimum, the following information should be documented in a PRA:

- A summary of all computer code calculations used as the basis for estimating plant-specific source terms for selected accident sequences, specifically identifying those with potential for large releases.
- A description of modeling methods used to perform plant-specific source term calculations; this includes a description of the method by which source terms are assigned to accident sequences for which computer code (e.g., MAAP or MELCOR) calculations were **not** performed.
- If analyses of a surrogate (i.e., "similar") plant are used (as a basis for characterizing any aspect of radionuclide release), transport or deposition in the plant being analyzed, references to, or copies of, documentation of the original analysis, and a description of the technical basis for assuming applicability of results.

3.2.3 Treatment of Source Term Uncertainties

Results of the Level 2 PRAs described in NUREG-1150 indicate that uncertainties associated with processes governing radionuclide release from fuel, transport through the primary coolant system, secondary coolant system (if applicable), and containment, and deposition on bounding structures, can be a major contributor to the uncertainty in some measures of risk.

Uncertainties in the processes specifically related to radionuclide source term assessment should, therefore, be represented in a Level 2 PRA. A systematic process and calculation tools to accommodate source term uncertainties into the overall evaluation of severe accident risks were developed for the Level 2 PRAs described in NUREG-1150. A detailed description of this process and the associated tools is not provided here and the reader is referred to NUREG/CR-4551, Vol. 2, Part 4 (Ref. 3.20), NUREG-1335, Appendix A (Ref. 3.19), NUREG/CR-5360 (Ref. 3.21), and NUREG/CR-5747 (Ref. 3.22) for additional information on these topics.

3 Internal Event Level 2 PRA for Full Power Operations

3.2.3.1 Considerations for the Baseline PRA

The areas in which key uncertainties are addressed in a Level 2 analysis are summarized below:

- Magnitude of radionuclide release from fuel during core damage and relocation of the released material in-vessel (primarily for volatile and semi-volatile radionuclide species).
- Chemical form of iodine for transport and deposition.
- Retention efficiency during transport through the primary and secondary coolant systems.
- Magnitude of radionuclide release from fuel (primarily refractory metals) and non-radioactive aerosol generation during corium-concrete interactions.
- Decontamination efficiency of radionuclide flow streams passing through pools of water (BWR suppression pools and PWR containment sumps).
- Late revaporization and release of iodine initially captured in water pools, and
- Capture and retention efficiency of aerosols in containment and secondary enclosure buildings.

When deterministic codes are being used to estimate the source term, it is important to account for all of the relevant phenomena even when the code does not explicitly include models for all of the phenomena. When a model is not available for certain important phenomena, it is not acceptable to simply ignore the phenomena. Instead, alternative methods, such as consulting different code calculations, using specialized codes, or assessing relevant experimental results, should be used.

When consequences are being estimated in the PRA, it is important to accurately represent the timing of the release. Past studies have shown that the number of early fatalities can be particularly sensitive to when the release occurs relative to when emergency response actions such as a general evacuation of the close-in population are initiated. Hence, it is also important that the approach used to estimate the source term properly accounts for timing characteristics of the release.

3.2.3.2 Application Impact Considerations

It is not likely that changes in a plant's CLB will impact the treatment of uncertainties in the radionuclide source term.

3.2.3.3 Interfaces with Other Tasks

The establishment of uncertainties in the radionuclide source term requires correct propagation of uncertainties through the accident progression.

3.2.3.4 Documentation

Documentation of analyses performed to characterize radiological source terms should provide sufficient information to allow an independent analyst to reproduce the results. At a minimum, a description of the method by which uncertainties in source terms are addressed should be documented for a quality PRA.

REFERENCES FOR CHAPTER 3

- 3.1 EPRI, "MAAP4 - Modular Accident Analysis Program for LWR Power Plants," RP3131-02, Vols 1-4, Electric Power Research Institute, 1994.
- 3.2 R. M. Summers, et al., "MELCOR Computer Code Manuals - Version 1.8.3," NUREG/CR-6119, SAND93-2185, Vols. 1-2, Sandia National Laboratories, 1994.
- 3.3 USNRC, "Uncertainty Papers on Severe Accident Source Terms," NUREG-1265, 1991.
- 3.4 F. T. Harper, et al., "Evaluation of Severe Accident Risks: Quantification of Major Input Parameters. Expert Opinion Elicitation on In-vessel Issues," NUREG/CR-4551, Volume 2, Revision 1, Part 1, Sandia National Laboratories, December 1990.
- 3.5 USNRC, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, December, 1990.
- 3.6 J. J. Gregory, et al., "Evaluation of Severe Accident Risks: Sequoyah, Unit 1," NUREG/CR-4551, Volume 5, Revision 1, Parts 1 and 2, December 1990.
- 3.7 T. D. Brown, et al., "Evaluation of Severe Accident Risks: Grand Gulf, Unit 1," NUREG/CR-4551, Volume 6, Revision 1, Parts 1 and 2, December 1990.
- 3.8 T. Blanchat and D. Stamps, "Deliberate Ignition of Hydrogen-Air-Steam Mixtures Under Conditions of Rapidly Condensing Steam", SAND94-3101C, 22nd Water Reactor Safety Meeting, Bethesda, MD, October 24-26, 1994.
- 3.9 C. K. Park, et al., "Evaluation of Severe Accident Risks: Zion Unit 1," NUREG/CR-4551, Volume 7, Revision 1, BNL-NUREG-52029, Brookhaven National Laboratory, March 1993.
- 3.10 R. J. Breeding, et al., "Evaluation of Severe Accident Risks: Surry Unit 1," NUREG/CR-4551, SAND86-1309, Vol. 3, Rev. 1, Part 1, Sandia National Laboratories, October 1990.
- 3.11 I. S. Basu, "An Overview of the Ex-Vessel Debris Coolability Issue," Presented at the 21st Water Reactor Safety Meeting (WRSM), Bethesda, MD, October 26, 1993.
- 3.12 R. E. Blose, et al., "SWISS: Sustained Heated Metallic Melt/Concrete Interaction with Overlying Water Pools," NUREG/CR-4727, July 1987.
- 3.13 W. W. Tarbell, et al., "Sustained Concrete Attack by Low Temperature, Fragmented Core Debris," NUREG/CR-3024, July 1987.
- 3.14 R. E. Blose, et al., "Core-Concrete Interactions with Overlying Water Pools - The WETCOR-1 Test," NUREG/CR-5907, November 1993.
- 3.15 B. W. Spencer, et al., "Results of MACE Tests M0 and M1," Proceedings of the 2nd CSNI Specialists Meeting on Molten Core Debris Concrete Interactions, Karlsruhe, Germany, Report No. NEA/CSNI/R(92)10, April 1992.

- 3.16 M. M. Pilch, et al., "The Probability of Containment Failure by Direct Containment Heating in Zion." NUREG/CR-6075, Sandia National Laboratories, 1994.
- 3.17 M. M. Pilch, et al., "Resolution of the Direct Containment Heating Issue for all Westinghouse Plants with Large Dry Containment or Subatmospheric Containment." NUREG/CR-6338, SAND95-2381, February 1996.
- 3.18 T. G. Theofanous, et al., "The Probability of Mark-I Containment Failure by Melt-Attack of the Liner." NUREG/CR-6025, November 1993.
- 3.19 USNRC, "Individual Plant Examination: Submittal Guidance." NUREG-1335, August 1989.
- 3.20 F. T. Harper, et al., "Evaluation of Severe Accident Risks: Quantification of Major Input Parameters." NUREG/CR-4551, SAND86-1309, Vol. 2, Rev. 1, Part 4: Experts' Determination of Source Term Issues, Sandia National Laboratories, 1992.
- 3.21 H-J. Jow, et al., "XSOR Codes User Manual." NUREG/CR-5360, SAND89-0943, Sandia National Laboratories, 1993.
- 3.22 H. P. Nourbakhsh, "Estimate of Radionuclide Release Characteristics into Containment Under Severe Accident Conditions." NUREG/CR-5747, BNL-NUREG-52289, November 1993.

4. INTERNAL EVENT LEVEL 3 PRA FOR FULL POWER OPERATIONS

This chapter provides attributes for a Level 3 probabilistic risk assessment (PRA) for accidents initiated during full power operations of a nuclear power plant. A Level 3 PRA evaluates the consequences of an accidental release of radioactivity to the environment. Therefore, those PRA applications (e.g., averted dose, impact of evacuation strategies on early fatalities, etc.) that need information on offsite consequences should include a Level 3 PRA. A Level 3 PRA is also needed if the application necessitates that numerical values for risk be determined (e.g., for comparison with the U.S. Nuclear Regulatory Commission's [NRC's] quantitative health objectives, QHO). Accidents initiated by internal events including internal fire and floods are addressed in the following section. Accidents initiated by external events are addressed in Chapter 5.

Analysis tasks performed as part of the Level 3 portion of a full-scope PRA consist of two major elements:

- accident consequence analysis, and
- computation of risk by integrating the results of Level 1, 2 and 3 analyses.

Attributes for an analysis in each of these areas are described below.

4.1 Accident Consequence Analysis

The consequences of an accidental release of radioactive material from a nuclear power plant can be expressed in several forms, for example, impacts on human health, the environment, and economic impacts. The consequence measures of most interest to a Level 3 PRA focus on impacts to human health. Specific measures of accident consequences developed in a Level 3 PRA should include:

- Number of early fatalities
- Number of early injuries
- Number of latent cancer fatalities
- Population dose to various distances from the plant
- Individual early fatality risk defined in the early fatality QHO (i.e., risk to the average individual within 1 mile of the site boundary)
- Individual latent cancer risk defined in the latent cancer QHO (i.e., risk to the average individual within 10 miles of the plant).
- Land contamination.

4 Internal Event Level 3 PRA for Full Power Operations

4.1.1 Considerations for the Baseline PRA

Several probabilistic consequence assessment (PCA) codes are currently in use for estimating the consequences of postulated radiological releases. The MACCS computer code⁴¹ is supported by the NRC for use in nuclear power plant Level 3 PRAs. An earlier version of this code was used in the analyses reported in NUREG-1150⁴².

The MACCS code necessitates a substantial amount of supporting information on local meteorology including windspeed, atmospheric stability, and precipitation, demography, land use, property values, etc. (Ref. 4.1 provides a complete description of the input data necessary). In a full-scope evaluation of accident consequences, this information should represent current, site-specific conditions.

In addition, MACCS requires that the analyst make assumptions on the values of several parameters related to the implementation of protective actions following an accident, for example:

- The (site-specific) time needed to warn the public and initiate the emergency response action (e.g., evacuation or sheltering).
- The effective evacuation speed.
- The fraction of the offsite population which effectively participates in the emergency response action.
- The degree of radiation shielding afforded by the building stock in the area.
- The projected dose limits assumed to trigger normal and hot spot relocation during the early phase of the accident.
- The projected dose limits for long-term relocation from contaminated land, and
- The projected ingestion doses used to interdict contaminated farmland.

Since the values assumed for the above parameters have a significant impact on the consequence calculations, the selected values need to be justified and documented.

4.1.2 Application Impact Considerations

It is unlikely that a change in a plant's current licensing basis (CLB) would effect the accident consequence assessment. However, if the application necessitates knowledge of a particular risk measure (e.g., population dose for cost-benefit analysis or individual risk for comparison to the NRC's quantitative health objectives) then the consequence model used should be able to calculate these parameters.

⁴¹D.I. Chanin, et al., "MELCOR Accident Consequence Code System (MACCS), User's Guide," NUREG/CR-4691, SAND86-1562, Sandia National Laboratories, 1990.

⁴²USNRC, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, December 1990.

4.1.3 Interfaces with Other Tasks

This task interfaces with the output of the Level 2 PRA and provides the magnitude of various risk measures conditional on a release occurring. The output of this task is used in the computation of risk (Section 4.2).

4.1.4 Documentation

Documentation of analyses performed to estimate consequences associated with the accidental release of radioactive material to the environment should provide sufficient information to allow an independent analyst to reproduce the results. At a minimum, the following information should be documented for a PRA:

- A description of the site-specific data and assumptions used to perform the consequence calculations.

4.2 Computation of Risk

The final step in a Level 3 PRA is the integration of results from all previous analyses to compute the selected measures of risk. The severe accident progression and the fission product source term analyses conducted in the Level 2 portion of the PRA, as well as the consequence analysis conducted in the Level 3 part of the PRA, are performed on a conditional basis. That is, the evaluations of alternative severe accident progressions, resulting source terms, and consequences, are performed without regard to the absolute or relative frequency of the postulated accidents. The final computation of risk is the process by which each of these portions of the accident analysis are linked together in a self-consistent and statistically rigorous manner.

4.2.1 Considerations for the Baseline PRA

The important attribute by which the rigor of the process is judged is the ability to demonstrate traceability from a specific accident sequence through the relative likelihood of alternative severe accident progressions and measures of attendant containment performance (i.e., early versus late failure) and ultimately to the distribution of fission product source terms and accident consequences. This traceability should be evident in both directions: i.e., accident sequence to a distribution of consequences and from a specific level of accident consequences back to the fission product source terms, containment performance measures, or accident sequences that contribute to that consequence level.

4.2.2 Application Impact Considerations

It is unlikely that a change in a plant's CLB would effect the method used to compute risk. However, if the application necessitates knowledge of a particular risk measure (e.g., population dose for cost-benefit analysis or individual risk for comparison to the NRC's quantitative health objectives) the risk integration model used should be able to calculate these parameters.

4.2.3 Interfaces with Other Tasks

This task interfaces with the output of the Level 1 and 2 PRA tasks and calculates various risk measures.

4.2.4 Documentation

Documentation of analyses performed to estimate risk should provide sufficient information to allow an independent analyst to reproduce the results. At a minimum, the following information should be documented for a PRA:

- A description of modeling methods used to assign consequences to individual accident sequences represented in the probabilistic logic model; this includes a description of the method by which the full spectrum of severe accident source terms generated as part of the uncertainty analysis are linked to a limited number of actual consequence calculations.
- A description of the computational process used to integrate the entire PRA model (Level 1 through Level 3).
- A summary of all calculated results including frequency distributions for each risk measure.

5. EXTERNAL EVENT PRA FOR FULL POWER OPERATION

The analysis of external events in a Probabilistic Risk Assessment (PRA) necessitates different considerations than those for an internal events analysis. This chapter discusses the attributes which should be considered in performing or reviewing a baseline external event PRA for full power operation. In addition, considerations for using the external event PRA models for evaluating the risk-significance of a proposed licensing modification are also presented.

5.1 Level 1 Analysis

This section presents the considerations for performing a Level 1 seismic PRA while at full power. In addition, considerations for performing a Level 1 PRA analysis of other external events which can be important at various plant sites (e.g., high winds, tornados, hurricanes, and nearby transportation accidents) are also presented. The evaluation of external event during lower power shutdown conditions is discussed in Chapter 6. Since the analysis of external events generally utilize the models generated for the internal events analysis, the considerations discussed in Chapter 2 are also applicable for these events. The PRA considerations presented in this section thus focuses on those Level 1 modeling aspects which are unique to the external events. However, the influence of the external events on the internal event Level 1 models (e.g., the impact of stress level, equipment accessibility, and lack of indications caused by an external event on the human reliability assessment) is also discussed.

5.1.1 Seismic Analysis

The objective of a seismic PRA is to analyze the risk due to core damage accidents initiated by earthquakes. This means that the frequency and severity of earthquakes should be coupled to models of the capacity of plant structures and components to survive each possible earthquake. The effects of structural failure should be assessed, and all the resulting information about the likelihood of equipment failure can be evaluated using the internal events PRA logic model of the plant modified as appropriate to include seismic-induced events.

The basic elements of a seismic PRA include (1) hazard analysis, (2) structure response analysis, (3) evaluation of component fragilities and failure modes, (4) plant system and sequence analysis, and (5) containment and containment system analysis.

This section highlights the major points to consider in the performance of a seismic PRA. Further details are contained in NUREG-1407 (Ref. 5.1) NUREG/CR-2300 (Ref. 5.2) and NUREG/CR-2815 (Ref. 5.3).

5.1.1.1 Considerations for the Baseline PRA

In a seismic PRA, seismic-induced failures in addition to random hardware failures are modeled. They can lead to accident initiating events as well as failures of components and systems that are needed to mitigate an accident. In an internal events PRA, usually only active components are modeled. In a seismic PRA, passive components, such as pipe sections, tanks, and structures, have to be included. Unique failure modes of these components have to be identified and added to the logic model. In addition, relay chatter is a unique component failure mode during an earthquake that should be addressed.

One important aspect of a seismic event is that all parts of the plant are excited at the same time. This means that there may be significant correlation between component failures, and hence, the redundancy of safety systems could be compromised. The correlation could be introduced by common location, orientation, and/or vibration frequency. This type of "common-cause" failure represents a unique risk to the plant that is reflected in a seismic PRA.

An additional consideration in the performance of a seismic PRA is the formation of both a well-organized walkdown team and a peer review team with combined experience in both system analysis and fragility evaluation. Ideally, the peer review should be conducted by individuals who are not associated with the initial evaluation to ensure ideally, both technical quality control and technical quality assurance of the PRA results and documentation.

5 External Event PRA for Full Power Operation

Identification of Structures, Systems, and Components to be Included in the Seismic Analysis

The systems, structures and components (SSCs) modeled in the internal events PRA, internal fire PRA (Section 2.3), and internal flood PRA (Section 2.2) can be used in the identification of potential seismic induced initiating events, component failure modes, and accident scenarios. They provide the starting point for the identification of SSCs to be included in the seismic analysis. In addition, a review of the fire and flood analyses can help identify the for potential for seismic-induced fires and floods. For example, failure of a heat exchanger or tank could lead to a flood that impacts other components. Similarly, rupture of an oil storage tank can cause a fire.

During the plant familiarization in preparation for performing a seismic PRA, plant documentation regarding equipment layout, design, and construction of the SSCs identified in the internal events PRA are typically reviewed. During this process, additional SSCs may be identified. During the plant walkdown, visual inspection of the equipment layout and component installation and anchoring should identify SSCs whose failure could impact the risk of the plant. The plant walkdown is critical to identify as-designed, as-built, and as-operated seismic weak links in plants. Information is gathered to determine the significant failure modes of the SSCs and if the failure of an SSC would impact other equipment needed to mitigate the accident. For example, failure of a structure could cause failure of equipment nearby due to falling debris. More detailed attributes for a walkdown can be found in Section 5 and 8 of the Electric Power Research Institute (EPRI) Seismic Margins Methodology (Ref. 5.4).

Initiating Events Analysis

Seismic-induced initiating events typically include transients, loss of offsite power (LOOP), and loss-of-coolant accidents (LOCAs). The postulated collapse of a major structure, such as the reactor building or turbine building, can be considered as an additional initiating event or as a basic cause for an initiating event that has been already identified in the internal events PRA. As mentioned previously, seismically induced fire and flood events can also be potentially identified. It is possible to have multiple initiating events for a given seismic event. This can be treated approximately by choosing the initiator with the worst impact from the standpoint of core damage probability and considering additional failures that are seismically induced. A systematic evaluation of the SSCs is performed to identify the causes of potential initiating events. In a manner similar to the way initiating events are grouped for an internal events PRA, the seismic failures can be grouped based on their impact on the plant. The results of the evaluation should produce a list of failures for each initiating event. The identified failures are then used to guide the quantification of the frequencies of the initiating events.

Hazard Analysis

In the 1980's, the methodologies for performing seismic hazard analysis were developed for the Eastern-U.S. sites by Lawrence Livermore National Laboratory (LLNL) (Ref. 5.5) and EPRI (Ref. 5.6). However, the seismic hazard curves by these two methodologies were significantly different for many of the eastern sites. As a result of the 1993 revision of the LLNL hazard curves (Ref. 5.7), either approach is currently considered to be acceptable. In 1993, an effort was also initiated to develop a method to produce more consistent seismic hazard curves (jointly supported by the NRC, EPRI, and the U.S. Department of Energy [DOE]). This recent development in seismic hazard analysis could also be used for future seismic PRAs. In the seismic hazard evaluation, site specific soil conditions should be incorporated into the site specific hazard curves to provide a true site-specific hazard evaluation. The potential for soil liquefaction should also be considered in a site-specific evaluation.

To quantify both the seismic hazard and component fragilities, a ground motion parameter needs to be selected. Traditionally, the peak ground acceleration or zero-period spectral acceleration has been used to represent the intensity of the earthquake hazard, which tends to introduce a significant uncertainty in the lower frequency range. To mitigate this problem, the average spectral acceleration is recommended for use since it expresses the ground motion intensity in terms of average response spectral values over the significant frequency range of interest for most structures and equipment (e.g., 5 Hz to 15 Hz). If an upper bound cutoff to ground motion at less than 1.5 g peak ground acceleration

is assumed, sensitivity studies should be conducted to determine whether the use of this cutoff affects the delineation and ranking of seismic sequences.

Fragility Analysis

The fragility of a component or structure is defined as the conditional probability of failure given a value of the ground motion parameter. All the potential failure modes, both structural and functional, need to be examined to quantify the fragility value of a component. The sources of information that can be used in a fragility evaluation include the plant-specific design and test data, available experimental results, experience in past earthquakes (e.g., for offsite power loss), and generic fragility values from past studies.

Generic fragility parameters can be used in the initial screening of components and structures. However, the appropriateness of the generic fragility parameters has to be verified during the plant walkdown as well as by reviewing the documentation on component and structure fragilities. The high-confidence-and-low-probability (HCLPF) value can be used to screen components and structures without quantification of the seismic fault trees or event trees. Screening using a specified g-level for components and structure can be used to eliminate components with higher HCLPFs from further consideration in the PRA. However, if the core damage frequency (CDF) results indicate significant importance of components at the specified g-level, then components screened at this level should be added to the model and the results recalculated.

In the final PRA model, all components and structures that appear in the dominant accident cut sets should have site-specific fragility parameters that are derived based on plant-specific information, such as anchoring and installation of the component or structure. The methodologies for fragility analysis are discussed in a number of references, for example, NUREG/CR-2300 and EPRI NP-6041. It is desirable to incorporate the results of the latest available test data into the analysis and to also include aging effects in the component and structure fragility evaluation.

Seismic Model Development and Quantification

Seismic event trees can be developed by modifying the event trees developed for the internal events PRA, as appropriate. The event trees should consider events that can occur during an earthquake including a LOOP, station blackout (SBO), other transients, and LOCAs of different sizes as well as multiple initiators. The fault trees developed for internal events can also be modified to include failures induced by earthquakes, as well as the impact of failed instrumentation or contradicting indications. The random failure and human errors included in the fault trees for the internal events analysis should be retained for the seismic analysis. Relay chatter and recovery actions can be included in the analysis using the information given in Section 3.1.1.4 of NUREG-1407.

The logic models should demonstrate that simultaneous failures of multiple SSCs (including a cross system boundary, if applicable) as a result of the earthquake are adequately modeled. Most of the seismic-induced failures can be adequately modeled by adding seismic-induced failure events in the fault trees for the affected systems. In terms of initiating events, a combination of multiple initiating events has to be considered. For example, a LOCA with simultaneous LOOP or SBO should be considered in the risk assessment.

The fault trees and event trees should be quantified with a sufficient number of g-values to cover the range of possible earthquake levels. For each g-value, the event trees are quantified to determine the conditional core damage cutsets and conditional core damage probability. Integration/summation of the products of the conditional core damage probability and the hazard curve over all g-values provides the overall CDF due to seismic events.

Quantification can be done in two or more iterations. The initial screening quantification can be done by partially using generic component fragilities. The final quantification should use site-specific fragilities for those components that appear in the dominant cutsets. Care should be taken to treat system successes and high failure probabilities properly by the computer algorithm used. The uncertainties in the results should be fully quantified and displayed.

5 External Event PRA for Full Power Operation

5.1.1.2 Application Impact Considerations

A particular change to a plant's current licensing basis (CLB) may influence the response of the plant to seismic events and thus influence the risk to the plant and public. The use of a seismic PRA in a risk-informed regulatory application necessitates that the impact of proposed plant or procedural changes be incorporated into the PRA evaluation. The actual nature of the impact will be application specific. However, in general, the proposed change should be evaluated for the impact on the following seismic PRA considerations.

- Identify if any additional SSCs should be included in the seismic model. Alternatively, the application may result in the removal of a SSCs from consideration.
- Review the impact of the proposed change on the identified seismic-induced initiating events including their grouping.
- The fragility of a component or structure may potentially be affected by a proposed change in a plant's CLB. The appropriateness of generic and plant-specific fragilities should be reviewed in light of a proposed change.
- The structure and quantification of developed event trees and fault trees used in the seismic PRA should be modified as appropriate to reflect the proposed plant modification.

5.1.1.3 Interfaces with Other Tasks

A seismic PRA can utilize the PRA models used to evaluate internal events. In general, the models are modified to include seismic-induced failures in addition to the random failures modeled in an internal event PRA. Thus, the performance of a seismic PRA necessitates interfaces with several internal event PRA tasks, including initiating event identification, accident sequence analysis, systems analysis, data analysis, and human reliability analysis (HRA).

5.1.1.4 Documentation

The documentation of a seismic PRA should be sufficient to enable a peer reviewer to reproduce the results. The process of identifying SSCs to be included in the seismic analysis should be documented. The process should be demonstrated to be systematic and complete. An example of a set of screening criteria are the attributes in Section 2 of the EPRI Seismic Margins Methodology (Ref. 5.4). A list of any SSCs that were screened out should be provided with the screening criteria/assumptions. A list of SSCs that were included in the seismic analysis should be provided, along with the findings and procedures of the plant walkdown.

The following information should be documented for each SSC:

- The type of component and the plant-specific identification number.
- The location and orientation of the component in the plant.
- Support and anchorage details.
- Evaluation results of possible seismic interactions.
- Inspection results on the condition of components and anchorages.
- Photographs (if appropriate), and
- Results of screening.

The screening criteria for seismically induced initiating events should be documented. The criteria should be consistent with those used in the internal events analysis. The quantification of seismically induced initiating events is documented with enough detail so that a knowledgeable reader could reproduce the quantitative results.

The description of the seismic hazard method should be provided, together with the information used to characterize the seismicity near the site, the local soil conditions and the potential for soil liquefaction.

The results of the seismic hazard analysis includes the seismic hazard curves for different confidence levels (typically for 5, 10, 20, 30, 40, 50, 60, 70, 80, 90, 95 percentile), and the corresponding response spectra. The seismic hazard should be quantified for both horizontal and vertical components.

The following information for documenting the seismic hazard evaluation should be considered:

- Description of the seismic hazard analysis method, including the identification of computer codes used in the analysis.
- If a plant-specific hazard analysis method is used, all the assumptions/parameters regarding the seismic zoning, source parameters of each seismic zone (magnitude-frequency relationship), attenuation formula and the local soil conditions.
- Hazard curves and the associated response spectra.

The methodologies used to quantify the fragility values of components, together with key assumptions, should be described sufficiently to allow for a peer review. A detailed list of the component fragility values should be provided that includes the method of seismic qualification, the dominant failure mode, source of information, and the location of the component. The fragility descriptors (median acceleration, uncertainty, and randomness) should be tabulated for all SSCs modeled, and the technical bases for the values used for each SSC should be provided.

Identification of the HCLPF values of all SSCs modeled is also recommended along with the basic fragility parameters. Both sequence-level and component-level HCLPF values should be provided to support decisions related to the identification and listing of seismic vulnerabilities.

The following information should be considered for documenting a fragility analysis:

- The description of the fragility analysis methodologies and key assumptions.
- Detailed fragility tables.
- Results of screening, and
- HCLPF values.

The following information on seismic model development and quantification should be documented:

- A description of the modeled initiating events including how SSC failures may cause the initiating events.
- A description of the seismic event trees with descriptions of the top events and seismic-induced failure events modeled. The modifications made to the event trees developed for the internal events PRA should be discussed in detail.
- The assumptions made related to correlated failures and how they were applied. For example, pumps from redundant trains of the same system are usually located in the same building and have the same orientation. Seismic-induced failures of pumps located in the same building are pessimistically assumed completely correlated unless more detailed analysis is performed to better quantify the correlation. A table containing all the correlated failures should be provided. The basis of the assumptions for correlations or lack thereof should be elaborated.
- The impact of structure failures. A table listing all the structures considered and the components or functions they affected should be provided.

5 External Event PRA for Full Power Operation

- Failures of components can lead to fire and flood in addition to loss of their functions. Detailed documentation of the evaluation of seismically induced fires and floods should be provided.
- Description of quantification methodology.
- A discussion of the risk profiles and dominant scenarios is for each earthquake magnitude.
- A discussion on considerations for uncertainties in seismic risk quantification. This should include the treatment of uncertainties for both hazard and fragility curves.

5.1.2 Analysis of "Other" External Events

Analysis of "other" external events for full power considerations should generally follow the processes already provided for full power analysis of internal event initiators. However, there are a few noteworthy differences that are discussed below.

5.1.2.1 Considerations for the Baseline PRA

The determination of what "other" external events need to be considered necessitates the review of many possible events that could occur. NUREG/CR-4839 (Ref. 5.8), for instance, provides a list of possible external events that should be considered for inclusion in this portion of the PRA.

This topic is further complicated by the fact that unlike the internal initiators, the "other" external events very often need to be described using a hazard curve rather than a single frequency estimate. This complicates the ability to screen out "other" external events on probabilistic grounds. Hence, screening of these events relies much more on sound deterministic arguments. The screening of any external events therefore necessitates adequate justification and documentation.

Modeling of accident sequences, equipment failures, and human errors generally follows the internal-events-full power attributes, except that spatial and plant layout factors become relevant as is the case for internal fire and flood events. For instance, structural and barrier considerations need to be included; equipment, barrier, and structural failures need to be modeled using fragility curves; new relevant failure modes and equipment operability issues need to be included in the analysis based on the effects of the external event; and the models should allow for appropriate combinations of external event-induced failures with the random failures already included in the internal events analysis.

Correspondingly, the data values (or curves) used for the failure probability of equipment, structures, barriers, and for human error should consider the effects of the external event as the hazard severity changes. This could mean that greater failure probabilities are used than in the internal events analysis.

Finally, the quantification aspects of the analysis necessitate a much more sophisticated analysis technique (and hence computer code capabilities and validation) in order to properly determine the CDF resulting from these "other" external events. This technique should integrate the full spectrum of hazard potential (as delineated by the hazard curve) and the spectrum of failure probabilities in the model (defined by fragility curves and other means to describe how failure probabilities of plant equipment and human errors change as a function of the hazard severity).

5.1.2.2 Application Impact Considerations

As with the case of the analysis of internal events (including fires and floods) and seismic events, a proposed change in a plant's CLB can potentially impact the risk from other external events. The actual nature of a proposed plant modification or procedural change will determine how the PRA evaluation of these other external events is impacted. In general, the following factors should be considered in the risk evaluation of such a change:

- The screening of other external events should be reviewed for a proposed modification to a plant's CLB to determine if the other external events considered or not considered in the baseline analysis are still appropriate.
- Potential changes to SSC fragilities resulting from the CLB change for the modeled external events should be considered.
- The potential for additional spatial-related failure mechanisms should be reviewed.
- Changes to the existing baseline PRA models and data (including HRA values) necessary to account for the CLB modification should be identified.

5.1.2.3 Interfaces with Other Tasks

The evaluation of other external events can utilize the PRA models used to evaluate internal events. The internal event models are modified to include additional failure modes induced by the external events. Thus, the analysis of other external events necessitates interfaces with the internal event PRA models, including primarily initiating event identification, accident sequence analysis, systems analysis, data analysis, and HRA.

5.1.2.4 Documentation

The following information should be considered for documenting a PRA analysis of "other" external events:

- A discussion of the process and the results of the screening of "other" external events.
- Details regarding how the retained events are modeled, particularly how the internal event models are modified for the analyses to include spatial impacts.
- A discussion of the external event hazard curves and the fragility curves for components and structures.
- A discussion on how the human error rates are impacted by the external events.
- The results of the analyses.

5.2 Level 2 Analysis

This section addresses some factors to consider when performing a Level 2 seismic PRA while at full power. It also provides considerations for performing a Level 2 PRA analysis for other external events (e.g., high winds, tornados, hurricanes, and nearby transportation accidents). In general, the considerations for performing Level 2 PRA for external events are the same as for an internal event Level 2 PRA. Thus, only those factors unique to external events are provided in the subsequent sections.

5.2.1 Seismic Analysis

As with the Level 1 portion of the seismic analysis, the Level 2 analysis should consider the impact of an earthquake on the core damage mitigating systems and the containment. The attributes for performing and documenting both the baseline and application-specific Level 2 portion of the seismic analysis includes the same considerations as discussed for the internal events analysis. In addition, the potential for an earthquake resulting in the failure of containment isolation valves to close, failure of containment spray systems, or failure of standby gas treatment systems all should be evaluated. This can be accomplished as is done in the Level 1 analysis by including seismic-induced failures in the internal events Level 2 models.

5 External Event PRA for Full Power Operation

5.2.2 Analysis of "Other" External Events

As with the Level 1 portion of the analysis of "other" external events, the baseline and application-specific Level 2 analysis should consider the impacts of the external events on the mitigation of core damage accidents. The impact of the identified external events on mitigating systems thus necessitates the same considerations as listed above for the other Level 1 analyses. In addition, any direct impacts on the containment from the external events should be evaluated and documented.

5.3 Level 3 Analysis

This section identifies some factors to consider when performing a Level 3 analysis of the consequences from external events that occur during full power operation. In general, the performance of the Level 3 analysis utilizes the same models used in evaluation of internal events. The major difference is in the consideration of the impact of external events on emergency response actions such as evacuation of the close-in population. It is unlikely that a CLB change would impact the Level 3 modeling.

5.3.1 Seismic Analysis

The attributes in Chapter 4 is also, in general, applicable for a seismic analysis. However, under some circumstances an earthquake can present conditions that would change the consequence assessment generated for the internal events analysis. In addition to changing the potential source terms, an earthquake can influence the ability of the population surrounding a plant to evacuate upon declaration of a general emergency. A Level 3 seismic PRA should, therefore, include consideration of the impacts of different levels of earthquakes on the consequence assessment (Ref. 5.9). A thorough discussion and documentation of the assumptions used in the consequence assessment should be provided.

5.3.2 Analysis of "Other" External Events

The impact on the Level 3 analysis should be included in the evaluation of other external events. The primary concern is the impact of the external events on the potential for evacuation. The attributes provided in Chapter 4 also apply for the Level 3 analysis of "other" external events. How any unique ways in which the external events might impact the Level 3 analysis should be evaluated and documented.

REFERENCES FOR CHAPTER 5

- 5.1 J. T. Chen, et. Al., "Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities," NUREG-1407, U.S. Nuclear Regulatory Commission, June 1991.
- 5.2 J. W. Hickman, "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," NUREG/CR-2300, Vols. 1 and 2, American Nuclear Society and Institute of Electrical and Electronic Engineers, January 1983.
- 5.3 M. McCann, et al., "Probabilistic Safety Analysis Procedure Guide," NUREG/CR-2815, Vol. 2, Revision 1, Brookhaven National Laboratory, August 1985.
- 5.4 "A Methodology for Assessment of Nuclear Power plant Seismic Margin," EPRI Report NP-6041, 1988.
- 5.5 D. L. Drenreuter, J. B. Savy, R. W. Mensing and J. C. Chen, "Seismic Hazard Characterization of 69 Nuclear Plant Sites East of the Rocky Mountains," NUREG/CR-5250, Lawrence Livermore National Laboratory, January 1989.
- 5.6 Electric Power Research Institute, "Probabilistic Seismic Hazard Evaluations at Nuclear Power Plant Sites in the Central and Eastern United States: Resolution of the Charleston Earthquake Issue," Prepared by Risk Engineering Inc., Yankee Atomic Power Company and Woodward Clyde Consultants, EPRI Report NP-6395-D, April 1989.
- 5.7 US NRC, "Revised Livermore Seismic Hazard Estimates for 69 Nuclear Power Plant Sites East of the Rocky Mountains," NUREG-1488, October 1993.
- 5.8 M. K. Ravindra, H. Banon, "Methods for External Event Screening quantification: Risk Methods Integration and Evaluation Program (RMIEP) Methods Development," Sandia National Laboratories, NUREG/CR-4839, July, 1992.
- 5.9 R. J. Breeding, et al., "Evaluation of Severe Accident Risks, Surry Unit 1," Sandia National Laboratories, NUREG/CR-4551, October 1990.

6. INTERNAL AND EXTERNAL EVENT PRA FOR LOW POWER AND SHUTDOWN OPERATIONS

The purpose of this chapter is to specify the necessary attributes of a full-scope probabilistic risk assessment (PRA) of low power and shutdown (LP&S) operating conditions. The tasks discussed are basically the same as those described in Chapters 2 through 5. This chapter will focus on any differences and/or additional tasks imposed by the analysis of LP&S conditions. However, note that it is not the intent of this discussion to prescribe how to perform a PRA for LP&S conditions.

For those LP&S tasks that are significantly different from those of full power operation, the differences and additional considerations are discussed for the baseline PRA. In addition, the potential impacts of risk-informed applications, interfaces with other tasks, and required documentation are discussed in separate sub-sections. For those LP&S tasks that are very similar to the tasks of full power operation, this fact is stated and references to the full power sections are made without further elaboration.

The scope of the LP&S analysis includes all plant operating conditions except for full power, which is described in Chapters 2 through 5. Examples of states included in an LP&S analysis are low power (e.g., power < 15%), hot shutdown/standby, cold shutdown, and refueling.

The risk associated with the operation of a plant in a particular operational state is estimated based on the average risk per year. Thus, the fractions of time associated with the operation of the plant in the various states should sum to 1.0. This implies that if the full power risk has been calculated based on being in full power operation for an entire year, then the results of the full power analysis should be reduced by the fraction of time the plant is not at full power on a per year basis (e.g., if the plant is at full power 70% of the time on a per year basis, the full power risk on a per year basis would be 0.7 times the originally calculated full power risk value). Likewise, the risk associated with any individual operating state should include the fraction of time the plant is in that particular plant operational state (POS).

For LP&S conditions, the fuel is assumed to remain in the reactor vessel. Risk associated with spent fuel stored in the spent fuel pool, and cases where fuel is partially or totally off-loaded to the spent fuel pool during refueling are considered out of the scope of this document.

Typically, the plant operating states of a refueling cycle can be grouped into four distinct categories:

- Power operation (i.e., full power operation).
- Controlled shutdown to below x% power (where x represents the transition point from low power to full power operations).
- Scram, and
- Refueling outage.

As stated previously, the analysis of full power operation is described in earlier Chapters 2 through 5. The analysis of "OK" sequences originating from a full power analysis are excluded from the LP&S analyses; thus, the fractions of time spent in operational states resulting from a plant scram are not included in the analysis of risk during LP&S.

6 PRA for Low Power and Shutdown Operations

The basis for this is the assumption that the mission time used in the full power analysis is sufficient to adequately cover the operation of the plant during these states and that the data used to determine component unavailabilities for full power conditions already accounts for the known component unavailabilities during these states.

This leaves controlled shutdowns and refueling outages. In both cases, plant-specific historical data and current operating procedures are used to determine both the fraction of time spent in these states and to determine the unavailability of equipment in each operating state.

6.1 Internal Events Level 1 Analysis

As stated in Chapter 2, a Level 1 PRA is comprised of three major elements. For LP&S conditions, an additional consideration should be added to the accident sequence delineation task of a PRA. The purpose of this addition is to subdivide the operating cycle of the plant into sufficient plant operational states (POSSs) to allow the analysts to adequately represent the plant as it transitions from one operating state to another. While the number of POSSs may vary from plant-to-plant owing to the different operational characteristics of the plants, the important concept is the subdivision of the operation cycle into sufficient detail to allow the PRA analysts to accurately represent the status of the plant both from a systems availability and a decay heat viewpoint.

6.1.1 Plant Operational States

The objective of the POS identification and quantification task is to subdivide the plant operating cycle into sufficient detail such that the analysts can represent the plant operating within specific POSSs and transitioning from one POS to another, and to determine the fraction of time spent in each POS.

6.1.1.1 Considerations for the Baseline PRA

Identifying POSSs

A POS is "a plant condition for which the status of plant systems (operating, standby, unavailable) can be specified with sufficient accuracy to model subsequent accident events" (Ref. 6.1). In addition to the status of plant systems, knowledge about the decay heat load, and thus changes in success criteria, is important when identifying the POSSs.

In an LP&S PRA, the plant's operating cycle is subdivided into different POSSs. The characteristics important to the identification of the POSSs are as follows:

- reactor power level,
- in-vessel temperature, pressure, and coolant level,
- equipment normally operating and required to maintain the current operating parameters, and
- changes in the decay heat load or plant conditions (e.g., raised water level with upper pools connected during refueling at a boiling water reactor [BWR]) that allow new success criteria.

Examples of POSSs for pressurized water reactors (PWRs) and BWRs can be found in NUREG/CR-6144 (Ref. 6.2) and NUREG/CR-6143 (Ref. 6.1), respectively. It is possible that some special tests and operational activities, that

are of relatively short duration, require that the plant be placed in a configuration that is very different from the normal configuration of a POS. Such a configuration may not need to be treated as a separate POS. However, such test configurations should be identified and their contribution to risk evaluated.

Determining POS Fractions

For each POS identified, detailed plant-specific information is collected, such that the time spent in each POS can be determined. To determine the POS fractions for a refueling outage, plant-specific information on the previous four refueling outages is collected. If less than four outages are available, then information from all outages except the first is used. For controlled shutdown POSs, the fractions are determined by collecting plant-specific information from the previous five years of operation. If less than five years are available, the data from all years are used.

Screening of POSs

Screening of POSs should be performed by identifying available diverse and redundant means of removing decay heat and mitigating accidents. Supporting deterministic analyses and quantitative screening risk calculations are used to provide justification for screening out a POS. For example, during refueling operation with the refueling cavity filled, calculations should be performed to demonstrate that time to core damage is very long in different postulated accident scenarios.

6.1.1.2 Application Impact Considerations

A change in the current licensing basis can affect this task in the following way:

- Changes in the frequency of outages.
- Changes in the number of POSs.
- Changes in the duration of the POSs, and
- Changes in the other parameters used in defining the POSs.

The potential for these changes has to be evaluated for each risk-informed change in the current licensing basis (CLB).

In evaluating the risk impacts of plant changes, the inclusion of contributions from LP&S provides a more complete risk assessment.

6.1.1.3 Interfaces with Other Tasks

This task defines the initial conditions of the plant to be analyzed in all the subsequent tasks. In this task, the key parameters are specified for each POS. In the subsequent tasks, further characterization of the POSs is needed to complete the assessment. A PRA model similar to that for full power operation is developed for each POS.

6.1.1.4 Documentation

The following information are documented for an LP&S PRA:

- A list or general description of the information sources used in the task.

6 PRA for Low Power and Shutdown Operations

- A discussion of the POSs identified during the task. The discussion should specifically define each POS and describe how each POS was determined.
- Assumptions that were made during the identification of the POSs. The bases for the assumptions and their impact on the final results are also discussed.
- A description of the configuration of the systems, including those that are needed for continuous operation in the POSs.
- The time history information used to determine the POS fractions, including the amount of time spent in each POS for each refueling and controlled shutdown outage.
- The fractions of time calculated for each POS for both refueling and controlled shutdown outages.
- A list of special tests and operational activities that significantly change the plant configuration of a POS.
- List of PRA changes from risk-informed applications.

6.1.2 Accident Sequence Initiating Event Analysis

The objective of the initiating events task is the same as that described in Section 2.1.1, with the exception that for those POSs where the reactor is already shutdown, the requirement for a reactor trip is eliminated; however, the possibility of recriticality events is considered.

The LP&S specific considerations are provided for identifying additional initiating events, excluding events from consideration, grouping the individual initiating events, and documenting the work only when they differ from or are in addition to those contained in Section 2.1.1.

In an LP&S PRA, all those internal events that cause an upset of normal plant operation (some of which require a reactor trip) with the subsequent need for core heat removal are identified as initiating events. These events fall into one of four categories as follows:

- Loss-of-coolant accidents (LOCAs) — For LP&S conditions, those events that result in a diversion of water from the reactor vessel to some location where the water is recoverable, plus pipe rupture events in operating systems connected to the reactor vessel where the inventory loss may or may not be recoverable, are considered.
- Transients — All full power events applicable to the LP&S conditions are considered.
- Decay Heat Removal Challenges — All events that result in the isolation or loss of the normally operating decay heat removal system during shutdown conditions are considered.
- Reactivity Excursions — All events that lead to inadvertent reactivity insertion or problems with flow instability where the core is operated with a local high power-to-mass-flow ratio are considered.

Special issues or scenarios - Scenarios and issues identified in existing studies should be included. For example, reactivity accident scenario identified in the French Study (EPS 900) (Ref. 6.3), low-temperature overpressurization, failure of cavity seal, and failure of thimble tube seals should be addressed.

In ensuring "completeness" in identifying all potential initiating events for an LP&S PRA, the analyst should perform an engineering evaluation considering all events as described in Section 2.1.1, plus the analyst should evaluate those events that are unique to or have happened during shutdown operational states. Table 4.1.2 of NUREG/CR-6143, Vol. 2 (Ref. 6.1) and Table 4.1.3 of NUREG/CR-6144, Vol. 2 (Ref. 6.2) contain lists of events that have been considered during previous LP&S analyses.

The considerations associated with excluding and grouping initiating events are the same as those provided in Section 2.1.1. In addition, application impact considerations, interfaces with other tasks, and documentation guidelines are similar to those discussed in Section 2.1.1 for full power operation.

6.1.3 Accident Sequence Analysis

For this task, considerations are provided for selecting the accident sequence model, establishing the success criteria, modeling the accident dependencies, and documenting the work only when they differ from or are in addition to those presented in Section 2.1.2.

In addition to the considerations described in Section 2.1.2, top events representing the fractions of time spent in different system configurations (e.g., fraction of time the primary containment is open or the fraction of time a specific decay heat removal system is operating) are required if such information is needed to model accident progression to core damage.

As discussed in Section 2.1.2, inclusion of operator actions in the models is important. Due to the nature of shutdown conditions, more reliance may be placed on operator intervention. Thus, particular care should be given to the incorporation of human actions in the development of the event tree structure used to model the plant's response to any particular initiating event. Plant operating procedures should be examined carefully to determine how they will impact the operator's response during an accident.

Given the time dependency of the decay heat load, an LP&S PRA will examine the systems for unique configurations that may prove successful during shutdown conditions (e.g., gravity injection, reflux cooling, and alternate decay heat removal system). If these system configurations are deemed success criteria, then the LP&S PRA will make use of the systems by further subdividing a POS into different *time windows*. These time windows, which could be represented by sub-POSSs, allow for more realistic assessments of the impact of the decay heat loads on accident scenarios. Regardless of whether these subdivisions are classified as time windows or sub-POSSs, the accident sequence models contained in an LP&S PRA will properly account for the differences introduced into the accident sequence progression models.

The considerations associated with the modeling of accident dependencies and documentation are the same as those provided in Section 2.1.2. In addition, application impact considerations, interfaces with other tasks, and documentation are similar to those discussed in Section 2.1.2 for full power operation.

6 PRA for Low Power and Shutdown Operations

6.1.4 Systems Analysis

The LP&S considerations are the same as those described in Section 2.1.3. It should be noted that during shutdown conditions the alignment of systems may be significantly different as compared to that of full power operation, many instruments and indications may not be available, and consequently a higher likelihood of human initiated accidents may occur.

6.1.5 Data Analysis

For this task, considerations are provided for identifying the data sources and models, selecting the data input needs, quantifying data parameters, and documenting the work only when they differ from or are in addition to those presented in Section 2.1.4.

For selecting data input, the only modifications to the considerations described in Section 2.1.4 are as follows:

- In reviewing incidents for potential initiators, all incidents that meet the definition of an initiating event as given in Section 6.1.2 are considered in an LP&S PRA. However, the frequency of these events will be different from the frequency at full power operation. Plant-specific operating experience during LP&S should be used to estimate the frequency of these events in each plant operating state.
- In reviewing the incidents on component performance, all incidents that could affect the performance of equipment during the POS are considered in an LP&S PRA. In quantifying equipment reliability parameters and common-cause failure probabilities, data from all plant operational states should be used to quantify these parameters as described in Section 2.1.4. However, each event should be considered to determine if there are conditions such that the probability or rate of the failure event would be different depending on the plant operational state.
- In quantifying component unavailability from test and maintenance, only incidents occurring during the POS are included in an LP&S PRA. Only plant-specific operational experience during LP&S operations should be used in estimating equipment unavailability. Additional consideration of concurrent unavailability and plant operational procedures during each POS, outage times for redundant equipment (both intra- and inter-system) should be examined and accounted for based on actual plant experience.
- It is very likely that in a selected POS the configuration of some systems and components changes. The fraction of time that a system or component spends in each possible configuration has to be estimated using plant-specific data supplemented with plant specific operation procedures and outage schedules.

Application impact considerations and interfaces with other tasks are similar to those discussed in Section 2.1.4 for full power operation. For documentation, the only additional information to be reported are the fraction of time associated with being in a particular POS, the conditional probability associated with being in a specific system configuration, and the information used to generate these values.

6.1.6 Human Reliability Analysis (HRA)

Given the increased dependence on the human for performing actions during shutdown conditions, human interfaces become even more critical in causing, preventing, and mitigating an accident than is the case during full power conditions.

The LP&S considerations are the same as those described in Section 2.1.5. It should be noted that during shutdown conditions, many systems may be in a configuration very different from those during full power operation; many instrumentation may not be available and a higher likelihood of human initiated accidents can exist.

6.1.7 Accident Sequence Quantification

The LP&S considerations are the same as those described in Section 2.1.6.

6.2 Internal Flood Level 1 Analysis

The purpose of this section is to describe the attributes of a state-of-the-art internal flood PRA for a plant during LP&S operations. Only those attributes that are unique to floods during LP&S operations are discussed. The PRA tasks that are the same as those for a full power internal flood PRA and LP&S internal events PRA are discussed in Sections 2.2 and 6.1, respectively.

The approach used in performing a full power flood analysis PRA can be used for an LP&S PRA flood analysis. However, the differences between LP&S and full power operation have to be accounted for in its application. The main differences between LP&S and full power operation are the initial conditions of the plant, definition of initiating events, and systems/functions needed to mitigate an accident. These are the subjects that are discussed in this section in terms of the key tasks of an LP&S internal flood PRA.

The considerations associated with the potential impacts of the changes in CLB, interfaces with other tasks, and documentation of an LP&S internal flood analysis are the same as those discussed for a full power PRA.

6.2.1 Definition and Characterization of POSS

A main difference between an LP&S internal flood PRA and a full power internal flood PRA is the initial conditions of the plant. The initial conditions defined and characterized in the LP&S internal events PRA, i.e., outage types and POSS, should be used in an LP&S internal flood PRA.

6.2.2 Initiating Event Analysis

A flood initiating event during LP&S conditions can be defined as a flood that causes an initiating event as defined in the LP&S internal events PRA.

The causes of internal floods identified in the full power internal flood PRA should be evaluated, taking into consideration the unique plant configuration and operating conditions during LP&S operations, to determine their applicability to LP&S conditions. For example, a pipe section that is a source of flood for full power operation may be isolated during shutdown conditions. If a source of floods is found applicable to LP&S conditions, the method of

6 PRA for Low Power and Shutdown Operations

quantifying its frequency used in the full power analysis should be reviewed for its applicability to LP&S conditions. For example, a pipe section that is a source of floods during full power operation may be subject to much lower pressure and temperature during shutdown. Therefore, the likelihood of its rupture may be significantly different from that of full power operation.

In addition to those flood sources identified in the full power internal flood PRA, a review of the shutdown configurations of plant systems and the operating procedures used during LP&S operations should be performed to identify unique sources of floods during LP&S conditions. A plant walkdown during shutdown should also be performed to identify such sources of floods.

6.2.3 Flood Propagation

The same approach as that used in a full power flood PRA can be used in an LP&S internal flood PRA. Flood propagation modeling includes estimating the quantity of water that may be involved, identifying the pathways and barriers for flood propagation, identifying the failure modes of the components that would be affected by the floods, and estimating the timing of the scenarios. The unique shutdown conditions of the plant have to be taken into consideration. For example, the refueling water storage tank (RWST) inventory during refueling operation may be significantly lower than that during full power operation and flood barriers including dams, floor plugs, and anti-reverse flow devices in drain lines may be removed during shutdown condition.

6.2.4 Flood Model Development and Quantification

LP&S internal flood event trees should be developed by modifying the event trees developed for the LP&S internal events PRA. The fault trees developed for the LP&S internal events PRA should be modified to account for the flood induced failures.

6.3 Internal Fire Level 1 Analysis

The purpose of this section is to describe the attributes of an internal fire PRA for a plant during LP&S operations. Only those attributes that are unique to fires during LP&S operations are discussed. The PRA tasks that are the same as those for a full power internal fire PRA and LP&S internal events PRA are discussed in Sections 2.3 and 6.1, respectively.

The approach used in performing a full power internal fire PRA can be used for an LP&S internal fire PRA. However, the differences between LP&S and full power operation have to be accounted for in its application. The main differences between LP&S and full power operation are the initial conditions of the plant, definition of initiating events, and systems/functions needed to mitigate an accident. These are the subjects that are discussed in this section in terms of the key tasks of an LP&S internal fire PRA.

The considerations associated with the potential impacts of the changes in CLB, interfaces with other tasks, and documentation of an LP&S internal fire analysis are the same as those discussed for a full power PRA.

6.3.1 Definition and Characterization of Plant Operational States

A main difference between an LP&S internal fire PRA and a full power internal fire PRA is the initial conditions of the plant. The initial conditions defined and characterized in the LP&S internal events PRA, i.e., outage types and POSs, should be used in an LP&S internal fire PRA.

6.3.2 Initiating Event Analysis

A fire induced initiating event during LP&S conditions can be defined as a fire that causes an initiating event as defined in the LP&S internal events PRA. For example, a fire that causes interruption of the residual heat removal (RHR) system is a fire induced initiating event. The definition of a fire induced initiating event should be used in the identification of critical fire locations of an LP&S PRA.

The fire frequency quantification should be performed in the same way it is done for full power operations. A fire incidence database including incidents during shutdown should be used. In reviewing the database, those events that are applicable to LP&S conditions should be identified.

6.3.3 Identification of Critical Fire Locations

A critical fire location for an LP&S condition is a location of a postulated fire that would lead to an initiating event and at the same time affect the systems and components needed to mitigate the accident. The approach developed in a full power fire PRA can be used in an LP&S fire PRA. The information collected during a full power fire PRA, including critical fire locations, provides useful background information for an LP&S PRA. However, in an LP&S PRA, a somewhat different set of systems and components needs to be taken into consideration, and the identification of critical locations has to be performed based on the definition of applicable initiating events. For example, loss of RHR can occur due to a fire that affects the RHR system or its support systems. Such a fire may not constitute an initiating event for full power operation. To identify possible fire locations, tracing of the cables for the components of these systems would be necessary. Similarly, the systems/functions needed to mitigate an accident during shutdown are not exactly the same as those needed for full power operation. Therefore, the critical fire locations of an LP&S PRA are not necessarily the same as those of a full power fire PRA.

6.3.4 Fire Propagation and Suppression

The same approach as that which was used in a full power fire PRA can be used in an LP&S internal fire PRA. However, the shutdown conditions of fire barriers and systems needed for detection and suppression of a fire should be taken into consideration. For example, a fire door being kept open during shutdown to facilitate movement of equipment will impact the propagation of a fire, and additional activities during shutdown may increase the likelihood of a fire being detected early.

6.3.5 Fire Model Development and Quantification

LP&S internal fire event trees should be developed by modifying the event trees developed for the LP&S internal events PRA. The fault trees developed for the LP&S internal events PRA should be modified to account for the fire induced failures.

6.4 Seismic Level 1 Analysis

The purpose of this section is to describe the attributes of an LP&S seismic PRA. Only those attributes that are unique to an LP&S seismic PRA are discussed. The PRA tasks that are the same as those for a full power seismic PRA and LP&S internal events PRA are discussed in Sections 5.1.1 and 6.1, respectively.

The approach used in performing a full power PRA can be used for an LP&S PRA. However, the differences between LP&S and full power operation have to be accounted for in its application. The main differences between LP&S and full power operation are the initial conditions of the plant, definition of initiating events, and systems/functions needed to mitigate an accident. These are the subjects that are discussed in this section in terms of the key tasks of an LP&S seismic PRA.

The considerations associated with the potential impacts of the changes in CLB, interfaces with other tasks, and documentation of an LP&S seismic internal fire analysis are the same as those discussed for a full power PRA.

6.4.1 Definition and Characterization of Plant Operational States

A main difference between an LP&S seismic PRA and a full power seismic PRA is the initial conditions of the plant. The initial conditions defined and characterized in the LP&S internal events PRA, i.e., outage types and POSs, should be used in an LP&S seismic PRA.

6.4.2 Initiating Event Analysis

A seismically induced initiating event during LP&S conditions can be defined as an earthquake that causes an initiating event as defined in the LP&S internal events PRA. The seismic-induced initiating events should include loss of offsite power (LOOP), loss of RHR, and LOCAs. Seismically induced fire and flood events should also be identified.

6.4.3 Identification of Structures, Systems, and Components (SSCs)

The SSCs to be considered in an LP&S seismic PRA should not be limited to those considered in the full power seismic PRA. This is due to the fact that the SSCs that either can affect an initiating event or are needed to mitigate an accident during LP&S operations are not identical to those considered in a full power seismic PRA. However, the same approach as that used in a full power seismic PRA can be used.

6.4.4 Hazard Analysis

The hazard analysis performed for a full power seismic PRA can be used.

6.4.5 Fragility Analysis

The fragility analysis of an LP&S seismic PRA should account for the shutdown-specific configuration of systems and components. For example, the RWST may be only partially filled during the refueling operation and its fragility would be significantly different from the case when it is full, and the steam generators are maintained at "wet layup" (filled with water) and their fragility would be significantly different from that of full power operation.

6.4.6 Model Development and Quantification

Seismic event trees for LP&S operations should be developed by modifying the event trees developed for the LP&S internal events PRA. The fault trees developed for internal events should be modified to include failures induced by earthquakes.

6.5 Level 1 Analysis of "Other" External Events

Much of what should be considered for "other" (e.g., high winds, tornados, etc.) external events during LP&S operation has already been covered in Section 5.1.2 of this report. The following covers additional considerations beyond those already included in that section.

The inclusion or exclusion of "other" initiating events needs to be re-examined and may need to be altered because of expected plant configurations or activities during LP&S operation. For instance, expected reconfiguration of some barriers (opening of doors normally closed during full power operation), introduction of temporary equipment such as scaffolding, periods of an open containment, fuel potentially in more vulnerable configurations than at full power, and introduction of new external hazards by personnel (e.g., caustic cleaning solvents, more vehicles onsite, etc.) are examples of why previously eliminated "other" external events may need to be reconsidered for analysis.

Similarly, the expected changes in plant configurations and equipment operability periods should be considered when modeling the possible mitigation pathways and hence the success and failure scenarios should an external event occur.

Additionally, the hazard frequencies need to be re-examined and may need to be changed in cases where they may be affected by plant personnel, such as greater vehicle use affecting the frequency of transportation accidents.

And finally, the data values (or curves) for both plant equipment failure and human errors need to be re-examined to account for such things as temporary installations, possible temporary degradation of equipment, less operability status indication for the operators, and detrimental effects for some human performance shaping factors (more noise, crowded conditions, etc.).

The considerations associated with the potential impacts of the changes in CLB, interfaces with other tasks, and documentation of an LP&S "other" external event analysis are the same as those discussed for a full power PRA.

6.6 Level 2 Analysis

The object of the Level 2 analysis is to assess the potential for release of radionuclides due to accidents during LP&S conditions.

6.6.1 Considerations for the Baseline PRA

Generally, the considerations provided in Chapter 3 for full power operation are also applicable to LP&S conditions. However, it should be noted that, just as the equipment required to prevent core damage during the Level 1 analysis can be affected by LP&S operating conditions, so too can the equipment considered during a Level 2 analysis. If certain recovery actions, e.g., restoration of RHR pumps, need to be performed inside the containment after bulk boiling of the reactor vessel inventory has commenced, the impact of environmental conditions inside the containment

6 PRA for Low Power and Shutdown Operations

on the chances of success of such actions need to be assessed. In addition, the containment may be open during certain shutdown POSs. These factors should be accounted for in the Level 2 analysis. Furthermore, care should be exercised when accounting for the physical and phenomenological differences associated with the characterization of radionuclide release during shutdown states.

The following are Level 2 considerations that should be evaluated:

- Level 2 systems – Containment systems, such as sprays, may not be required in some of the shutdown POSs. As a result, they may be out of service for extended periods of time. The status of such systems should be identified.
- Containment status – In some shutdown POSs, containment closure is not required. As a result, personnel hatches, equipment hatches, and containment penetrations may be left in an open position. The probability of an initially open containment has to be taken into consideration in the Level 2 analysis. The possibility that the operator would re-establish containment integrity subsequent to an accident initiating event has to be evaluated. Consideration should be given to the status of electric power, equipment, and material needed to re-establish containment integrity.
- Decay of radioactive isotopes – The impact of low decay heat levels on accident progression in LP&S POSs and the decay of short-lived radioactive isotopes which impact early health effect should be properly accounted for.
- These key uncertainties are derived, in part, from the results of the LP&S PRAs (Refs. 6.1 and 6.2) as well as more recent statements of key source term uncertainties published by the NRC for light-water reactor licensing purposes (Ref. 6.4). Configurations where air can enter the reactor vessel, such as when the vessel head has been removed for refueling, have been postulated to cause an enhanced release of certain radionuclides. The effect that air ingress has on the source term in such configurations needs to be assessed and, if important, included in the Level 2 model.

6.6.2 Application Impact Considerations

The considerations in assessing the risk impact of a change in the CLB are the same as those discussed in Chapter 3 for full power operation. In addition, the impacts on the shutdown specific issues discussed in Section 5.3.1 should be evaluated.

6.6.3 Interfaces with Other Tasks

The interfaces between a Level 2 LP&S analysis and Levels 1 and 3 analyses are the same as those for full power operation.

6.6.4 Documentation

The documentation requirement of a Level 2 LP&S analysis is the same as that of a Level 2 analysis of full power operation.

6.7 Level 3 Analysis

The discussions provided in Chapter 4 for full power operation are also applicable to L.P.&S conditions

REFERENCES FOR CHAPTER 6

- 6.1 D. Whitehead, et al., "Evaluation of Potential Severe Accidents during Low Power and Shutdown Operations at Grand Gulf, Unit 1," NUREG/CR-6143, SAND93-2440, Sandia National Laboratories, 1994.
- Volume 1: Summary of Results
- Volume 2: Analysis of Core Damage Frequency from Internal Events for Operational State 5 During a Refueling Outage
- Volume 3: Analysis of Core Damage Frequency from Internal Fire Events for Plant Operational State 5 During a Refueling Outage
- Volume 4: Analysis of Core Damage Frequency from Internal Flooding Events for Plant Operational State 5 During a Refueling Outage
- Volume 5: Analysis of Core Damage Frequency from Seismic Events for Plant Operational State 5 During a Refueling Outage
- Volume 6: Evaluation of Severe Accident Risks for Plant Operational State 5 During a Refueling Outage
- 6.2 T-L. Chu, et al., "Evaluation of Potential Severe Accidents during Low Power and Shutdown Operations at Surry Unit-1," NUREG/CR-6144, BNL-NUREG-52399, Brookhaven National Laboratory, 1994.
- Volume 1: Summary of Results
- Volume 2: Analysis of Core Damage Frequency from Internal Events during Mid-loop Operations
- Volume 3: Analysis of Core Damage Frequency from Internal Fires during Mid-loop Operations
- Volume 4: Analysis of Core Damage Frequency from Internal Floods during Mid-loop Operations
- Volume 5: Analysis of Core Damage Frequency from Seismic Events during Mid-loop Operations
- Volume 6: Evaluation of Severe Accident Risks during Mid-loop Operations
- 6.3 EPS 900, "A PSA for the Standard French 900 MWe PWR," Main Report, April 1990.
- 6.4 L. Soffer, et al., "Accident Source Terms for Light-Water Nuclear Power Plants," Final Report, NUREG-1465, U.S. Nuclear Regulatory Commission, 1995.

APPENDIX A. PRIORITIZATION OF SSCS AND HUMAN ACTIONS

A.1 Introduction and Objective

The objectives of this appendix are two fold. The first objective is to discuss the role of importance measures within the risk-informed regulatory framework. This is necessary because the framework does not explicitly rely on risk-ranking methods for the acceptance of the proposed regulatory modifications. The second objective is to provide discussions on the following three areas:

- methods and limitations of quantitative prioritization,
- techniques for qualitative prioritization, and
- attributes of an integrated approach to prioritization in support of risk informed applications.

Prioritization is typically performed both quantitatively and qualitatively. Quantitative prioritization is done based on probabilistic risk assessment (PRA) and by use of quantitative importance measures. Qualitative prioritization are done based on the defense-in-depth concept and by use of both PRA information and current deterministic safety considerations. Regardless of the specific regulatory application, prioritization can be conducted as an intermediate step to differentiate between the high safety significant^(A.1) and low safety significant components (HSSCs/LSSCs). Relaxing requirements for LSSCs is expected to have less aggregate risk impact than if requirements are relaxed for HSSCs. This application of ranking (e.g., relaxing requirements for LSSCs) does not guarantee that the acceptance criteria are met. However, importance measures can be used as a part of a systematic process of adding and removing components from the LSSC list.

Risk ranking provides an information base that can be used for implementation and monitoring phases of risk-informed and performance-based regulatory alternatives as discussed in Section 2.5 of DG-1061^(A.2). This is especially important in those applications where the risk impact of the proposed changes in requirements cannot be accurately estimated. Qualitative engineering and operational reasoning along with a database of the importance measures can be used to help justify proposed changes to the current licensing bases. If the importance analysis indicates that a particular SSC is an HSSC, then it probably is; on the other hand, if the importance analysis indicates that the SSC is not important, then this conclusion should not be accepted without careful investigation of the reasons.

The remainder of this appendix discusses the theoretical bases and physical interpretations for various importance measures. It also discusses the use of importance measures in risk prioritization and identifies their potential limitations. This general guidance is tailored to support specific applications, as appropriate, and may be further described in application-specific guides.

^{A.1}Letter from A. Thadani (NRR Associate Director for Technical Review) to C. Pipton (Vice President, NEI).
^{A.2}Terminology for Categorizing Systems Components and Structures in Risk-Informed Regulatory Applications," dated May 8, 1996.

^{A.3}USNRC, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decision on Plant-Specific Changes to the Current Licensing Basis," Draft Regulatory Guide DG-1061, February 1997.

A.2 PRA-Based Importance Assessment

Several different importance measures are typically calculated on the basis of PRAs^{(A.3)(A.4)}. Some importance measures use the numerical risk information contained in PRAs; these are referred to as quantitative importance measures. Quantitative importance measures typically determine the change in risk measures associated with the failure or success of equipment or human actions. Here, risk measures refer to both core damage frequency (CDF) and large early release frequency (LERF). By contrast, PRA-based qualitative importance measures do not use the risk contribution information, rather they use the logic information contained in PRAs. Qualitative importance measures typically determine the reduction or increase in the number of layers of defense against an accident as a result of the failure or success of equipment or human actions.

Definitions of various importance measures, their formulation, physical interpretation, and limitations are discussed in this section. Various sensitivity analyses are suggested to account for the known limitations^(A.5) in using the results of various importance measures. Some considerations for grouping of various equipment using the calculated importance measures are summarized.

A.2.1 Quantitative Importance Measures

A.2.1.1 Definitions of Importance Measures

Fussell-Vesely (FV) and Risk Reduction Worth (RRW) Importance Measures

An important element of the results of a PRA is the sorted list of the accident sequence minimal cutsets. For those applications where PRA assumptions and data are not challenged, the ranked list of minimal cutsets could provide a means for prioritization. In some applications where PRA assumptions, model, and data may be questioned (e.g., previously unrecognized motor-operated valve [MOV] failure modes in MOV testing applications), the PRAs may first have to be updated.

The ranked list of accident sequence minimal cutsets provides important insights concerning the combination of failure events that contribute to core damage and public risk. This information could be used to establish defenses against the major risk contributors. A ranking scheme using the minimal cutset contribution is the most straightforward. Since the minimal cutsets are sorted on the basis of their frequencies, one may decide to identify all components within the scope of the application that also show up in the dominant minimal cutsets. Depending on the application, the dominant minimal cutsets could be determined based on their total contribution to risk (e.g., account for 95 percent of the CDF for all initiators from internal and external events including shutdown PRA). Ranking based on minimal cutset contributions is typically performed in order to focus resources and refine the requirements to gain a significant safety benefit.

^{A.3}W. E. Vesely and T. C. Davis, "Evaluation and Utilization of Risk Importances," NUREG/CR-4377, August 1985.

^{A.4}W. E. Vesely, M. Belhadj, and J. T. Rezos, "PRA Importance Measures for Maintenance Prioritization Applications," *Journal of Reliability Engineering and System Safety*, Vol. 43, pp. 307-318, 1994.

^{A.5}W. E. Vesely, "The Use of Risk Importances for Risk-Based Applications and Risk-Based Regulations," *Proceedings of the PSA '96*, Park City, Utah, September 29-October 3, 1996.

The major deficiency with this ranking scheme is its poor discrimination capability. For example, a component that belongs to a cutset contributing 5 percent to the CDF will be ranked higher than a component that may belong to several minimal cutsets each contributing 1 percent or less to core damage, even though the net contribution of all of these cutsets could be more than 5 percent. To overcome this deficiency, specific importance measures known as the FV measure and RRW have been developed.

The FV measure is defined by the probabilities of the cutsets containing an event divided by the sum of all cutsets. Mathematically, the FV measure is calculated by the change in risk when the component is unoperational minus the risk when the component is operational over the baseline risk multiplied by the component unavailability. That is,

$$FV = P(x)[E(R|x=1) - E(R|x=0)]/[E(R)]$$

where $P(x)$ is the unavailability of component "x," $E(R)$ is the baseline expected risks, and $E(R|x=1)$ and $E(R|x=0)$ are conditional expected risks when the component x is unoperational and operational, respectively. The conditional and the unconditional expected risk are related based on the following probabilistic equation:

$$E(R) = P(x)E(R|x=1) + (1 - P(x))E(R|x=0)$$

Substituting the auxiliary probabilistic equation for the FV equation would yield the following result:

$$FV = 1 - [E(R|x=0)/E(R)] = 1 - (1/RRW)$$

where RRW in the second term in the right-hand side of the equation is known as the RRW importance measure. Therefore, the FV and RRW measures are closely related.

Either FV and RRW perform the same function as ranking based on minimal cutset contributions, but do so in a more refined manner. The primary objective of these importance measures is to identify components within the scope of the application that can result in the greatest risk benefit if more resources are allocated to improve their reliability. An example to illustrate the use of FV and RRW measures for relaxing requirements is discussed below.

The FV and RRW importance measures can be used to justify relaxation of requirements when the effect of relaxing requirements can be estimated in terms of component reliabilities. However, in this case, the analyst should first assume that the requirements are relaxed for all components within the scope of the regulatory requirement. The impact of such relaxation on component reliabilities should then be estimated, and the PRA input data should be updated. The use of the FV measure with the new baseline PRA can also identify components for which the requirements should not be relaxed. Relaxation of the requirements for the remaining components could then be justified. In the latter approach, the impact of the requirements is integrated into the ranking analyses.

Birnbaum Measure (BM) and Risk Achievement Worth (RAW)

The BM is simply the contribution of all cutsets involving an event x divided by the nominal unavailability of that event. Mathematically, a single component BM is defined by:

$$BM(x) = E(R|P_x=1) - E(R|P_x=0)$$

where $E(R|P_x=0)$ and $E(R|P_x=1)$ are the expected risks when the unavailability of component x is set to zero and one, respectively.

The BM and RAW measures are closely related. By dividing the above equation with the nominal expected risk, the following relationship is obtained

$$[BM(x)/E(R)] = RAW(x) - (1/RRW(x))$$

where $RAW(x)$ is the RAW for x , and it is defined by the expected risk when the unavailability of component x is set to one divided by the expected nominal risk value. Since RAW is usually much greater than one and RRW is usually very close to one (but always greater than one), an approximate relationship for BM would be as follows:

$$BM(x) \approx E(R) \cdot [RAW(x) - 1]$$

This equation shows the close relationship between RAW and BM. However, it should be noted that the BM is an absolute measure and it is not normalized with the expected risk ($E(R)$). This is in contrast with all other importance measures discussed so far (FV, RRW, and RAW), which are normalized by the expected risk. Use of absolute measures would facilitate the comparison of importance results for different sensitivity runs within a plant.

A fundamental probability relationship between the BM measure and the change in the expected risk as a result of a change in component unavailability can be established using the following relationship:

$$\Delta E(R) = BM(x) \cdot \Delta Q(x)$$

where $\Delta E(R)$ and $\Delta Q(x)$ are the changes in the expected risk and the unavailability of the component x .

A.2.1.2 Considerations in Calculating Importance Measures

The theoretical bases of various importance measures and their physical interpretations were discussed earlier. The basis of the importance measures were discussed independent of the application. This section discusses practical considerations for calculating the following component-level importance measures:

- truncation limit.
- completeness of risk models.
- measures of risk.
- component failure modes.
- implicit contributors.
- explicit dependencies, and
- implicit dependencies.

Consideration of Truncation Limit

The truncation limit is an important aspect of a risk evaluation and, therefore, plays an important role in the ranking process. Some PRA codes are designed to provide an upper bound estimate on the frequency of the truncated cutsets. These codes typically accumulate the frequencies of the cutsets truncated in a residue bin. Therefore, it would be easy to identify the fraction of risk (e.g., CDF) captured given a probabilistic truncation limit. Truncation limits should, therefore, 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 generally translate into a cutset truncation limit from $1.0\text{E-}12$ to $1.0\text{E-}8$ (per year).

Another important consideration for determining a truncation limit is imposed by the FV measure and ranking criteria. As an example, if the numerical cutoff criteria of 0.1 percent (0.001) is proposed for the FV importance measure, a truncation limit with enough resolution for estimating a FV of 0.001 should be at least 1000 times smaller than the total calculated risk (or CDF). This would ensure the survival of at least one minimal cutset after truncation with a contribution of 0.1 percent of total CDF. However, the FV measure for a component is the summation of the contribution of all minimal cutsets containing that component; therefore, it would be important for more than one minimal cutset to survive the truncation. This would require that the truncation limit be lowered at least by a factor of 10 to ensure appropriate coverage.

The third consideration for determining a truncation limit deals with the extent to which the basic PRA events are covered by the PRA-generated minimal cutsets that survive the truncation limit. PRAs typically model up to a couple of thousands of basic events. Depending on the truncation limit, some of these basic events may not show up in the final minimal cutsets generated by the PRA (i.e., those that survive the truncation limit). The importance measures associated with these basic events then cannot be evaluated. The truncation limit, therefore, must be selected such that the fraction of basic events not accounted for in the final list of minimal cutsets is less than 10 percent of all basic events. This truncation limit criterion could be application dependent. For example, in in-service testing (IST) application, 90 percent of all basic events related to pumps and valves modeled in the PRA may correspond to a truncation limit of $1\text{E-}11$. However, to satisfy the same criteria for graded QA may require a much lower truncation limit (which may not be practical). Application-specific truncation criteria are re-visited in each application-specific guide.

In summary, three requirements should be met for selecting a probabilistic truncation limit for the purpose of risk-based ranking:

- The truncation limit should be low enough to capture a large fraction of risk measures (e.g., at least 95 percent of the CDF and LERF).
- The truncation limit should be low enough to ensure capturing components within the range of FV criteria of interest (e.g., 10^{-4} multiplied by the total estimated CDF and LERF).
- The truncation limit should be low enough to account for at least 90 percent of all basic events in the final set of minimal cutsets. This criterion may be too restrictive, and depending on the application may need to be modified.

Completeness of the Risk Model

Importance measures may be calculated based on a portion of the risk (e.g., for internal events at full power) or the overall plant risk (internal and external events including shutdown risk). Depending on the completeness of the risk model, qualitative assessments (safety based) should be utilized for portions of the plant operation not included in the PRA assessment. When the importance measures are calculated, care should be taken in accounting for all contributors to the importance measure as well as the appropriate normalization (consistent with the PRA scope). When importance measures need to be calculated for overall risk, the results could be tabulated to show specific contributors to the importance measures from the PRA scope (internal, external, etc.) along with the overall importance measures.

Considerations of Measures of Risk

Importance measures can be calculated for various risk measures (e.g., CDF, containment failure probability, and release category frequency). Currently, importance measures are calculated for CDF and LERF. LERF covers all scenarios involving early containment failure and containment bypass. Importance measures (both normalized and non-normalized) calculated at different PRA levels cannot be combined (summed).

Consideration of Component Failure Modes

A component can perform several different functions, each with its own unique failure modes modeled in a PRA. For example, failure to open and re-close could be two different failure modes modeled in a PRA for an MOV. Importance measures can be calculated for all failure modes. Care should be taken in evaluating the overall importance of a component (to avoid missing some failure modes). The overall component importance measure and the contribution of each of its failure modes to the overall measure could be tabulated. Here, a combined measure could be used as the overall importance measure.

Consideration of Implicit Contributors

Many components are not explicitly modeled in PRAs; however, their risk contribution is implicitly accounted for. For example, many components in the balance of plant are not explicitly modeled in the PRA, but their risk contributions are implicitly accounted for through the frequency of initiating events. Some importance measures could be calculated for the implicitly modeled components. For a component not explicitly modeled in the PRA, the analyst should first identify those basic PRA events that could be affected by the failure or success of the given component. In the second step, the analyst should determine the contribution of the implicitly modeled component to the unavailability of the explicitly modeled PRA basic events. For example, the importance of the rupture of a pipe segment not included in the model could be evaluated based on the failure of the modeled component located in that segment. For those cases where such evaluation could not be performed quantitatively, qualitative evaluation discussed later in this appendix could be used. The above 2-step analysis would provide sufficient information for calculating all types of importance measures discussed earlier for a component that is implicitly modeled in a PRA.

Consideration of Explicit Dependencies

Various types of dependencies are explicitly accounted for in PRAs. For example, common-cause failures (CCFs) are sometimes explicitly accounted for through use of CCF parameters (such as beta factors). Importance measures calculated for a component should account for the contributions from the explicit dependencies. In most cases, PRAs are structured such that these dependencies could be easily accounted for in calculating importance measures.

(specifically TV measure); however, this is not always the case. Care should be taken to ensure that all dependency contributors are accounted for and the results of importance measures are tabulated to show the individual dependency contributions.

Consideration of Implicit Dependencies

Various dependencies are implicit in PRAs. For example, many transducers are explicitly modeled in PRAs as a part of actuation logic and can also provide information needed for successful manual action. On the other hand, some instrumentation, monitors, or fault indicators may not be modeled in the PRA. Information from these items may be needed for successful recovery actions. Care should be given to consider their impact on other (explicitly modeled) basic events.

A.2.2 Qualitative Importance Measures

Rank-based qualitative risk ranking (QRR) is sometimes performed to show that defense-in-depth would not be compromised as a result of changes in requirements or design. There are two types of qualitative ranking designed explicitly to address the defense-in-depth concept. These are minimal cutset ranking (MCR) and minimal pathset ranking (MPR). Since in most cases these two methods provide consistent results, only the MCR method will be discussed here. A simplified system block diagram (Figure A.1) is used to facilitate the discussion of this ranking method.

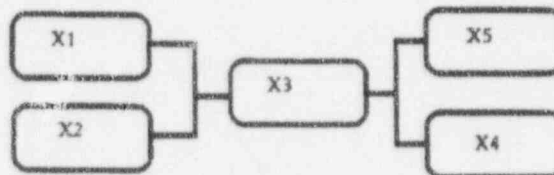


Figure A.1 Example system block diagram for discussion purposes

Minimal Cutset Ranking (MCR)

The MCR method ranks components based on the lowest order of the minimal cutsets when the component is removed. The lowest order of the minimal cutsets (number of elements in the minimal cutset) associated with the above system (Figure A.1) is one, and there is only one minimal cutset of order one (failure of X3 will render the system inoperable). If component X3 is removed, the lowest order of the minimal cutsets would be zero. However, if any other component (e.g., X1, X2, X4, or X5) is removed, the lowest order of minimal cutsets would be one and, in all cases, there would be two minimal cutsets of order one. Therefore, we infer that X3 is structurally more important than other components. The following procedure is typically used for MCR:

- For each component or basic event, the minimum order of cutsets (m) and the number of unique minimal cutsets with that order (n) is determined when the basic event is set to true. For this application, the order

of cutsets is determined by excluding all recovery actions and the initiating events (i.e., the cutset rank is based only on component failures).

- The components are then ranked based on the increasing values of m (i.e., the lowest order of minimal cutsets). For those basic events that have the same value of m , the ranking would be based on the decreasing value of n (the number of minimal cutsets with the lowest order). This step is typically done for each initiator separately.

MCR is a qualitative method and does not rely on the probability or quantitative risk as a result of removing a basic event from consideration. It can be used as a supplemental justification for quantitative importance ranking.

A.2.3 Considerations for Ranking Using Importance Measures

One application area considered for use of importance measures is risk ranking. Risk ranking applications involve relative ranking of all components based on their importance measures, and subsequent binning of the components in two (high and low) or three (high, medium, and low) classes. The binning is usually performed to allocate resources commensurate with component grouping. This may also result in enhancing the requirements for the components in the high bin category and may relax requirements for components in the low bin category. In this regard, care should be taken to ensure that relaxing requirements for components in the low bin category could not potentially degrade plant safety or multiple lines of defense.

The remainder of this section identifies special considerations for risk ranking, including those resulting from limitations of importance measures pertaining to ranking applications. This section also provides recommendations to deal with following issues in order to ensure that the components in the low bin category will not degrade safety:

- multiple component considerations.
- consideration for defense-in-depth.
- consideration for allowable plant configurations.
- consideration for binning criteria, and
- consideration for uncertainty evaluation.

Multiple Component Considerations

For those components assigned to the low risk category, the aggregate impact of changes in requirements of multiple components on safety should be assessed. For example, a set of MOVs may be in a low category since each MOV individually does not have a significant importance measure. If the requirements for this set of MOVs are changed, however, the failure rate of each individual MOV may increase. The aggregate impact of the increased failure rates for all MOVs might contribute significantly to risk. The underlying reason could be the appearance of some combination of these MOVs in the same cutset. The multiple component analysis is designed to identify which combination of these MOVs might be risk significant (therefore, requiring them to be shifted to a higher category). It should be emphasized that this concern about multiple components is also valid for components of different types, as long as they show up in the same cutset and are assigned to the low risk category. One acceptable way to address this issue is to identify all minimal cutsets containing at most one component from other categories (high or medium). If such a minimal cutset exists, some of the low category components should be moved to a higher bin to ensure that at least two or more higher category components are in all minimal cutsets.

Consideration for Defense-in-Depth

The following sensitivity analyses are recommended to ensure that multiple lines of defense are not degraded and defense-in-depth concept is not compromised as a result of relaxing the requirements on the low category components:

- Ensure that all minimal cutsets contain at least two component failures for which requirements are not relaxed. This ensures that there are at least two lines of defense in each cutset not affected by the regulatory change. (Either outside the scope of the application or categorized as medium or high.)
- Identify sets of contributors associated with major lines of defense, primary pressure boundary, safety functions, and containment systems. Prioritize the contributors within each set to assure a balanced coverage of all lines of defense.

Consideration for Allowable Plant Configurations

Plant Technical Specifications (TS) 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 these remaining components are assigned to the low category, their high reliability may not be ensured. The following analyses could be performed to ensure that multiple lines of safety are maintained during all allowable configurations.

The applicant should first identify those configurations that are allowed by plant TS that result in accident sequence minimal cutsets composed entirely of components categorized as LSSC (excluding the initiator). Such configurations should be prevented, or some of the low category components should be moved to the high category to ensure that no minimal cutsets totally rely on low category components during such configurations.

Consideration for Binning Criteria

The cutoff criteria for binning components based on their importance measures may vary from one application to another. Nonetheless, these criteria should be determined such that the total risk increase as a result of relaxing requirements for low category components are controlled. As an example, relaxing certain requirements could increase the unavailability of the affected components at most by a factor of 2. At the same time, the total risk increase as a result of such relaxation is planned to be controlled under 10 percent of the baseline core damage frequency. The binning criteria then should assure that the contribution of all basic events assigned to LSSC bin when their unavailabilities are increased by a factor of 2 stays below the 10 percent of the baseline CDF. The binning criteria, therefore, could vary depending on the application and the expected changes in the unavailabilities of the affected components.

The above procedure and criteria for binning are more appropriate than cutoff criteria based on an individual FV measure. This process also explicitly accounts for the impact of the relaxation in terms of increasing the component unavailability; therefore, the cutoff criteria can vary from one application to another (and even within a specific application) depending on the extent of relaxation requested.

Considerations for Uncertainty Evaluation

The effects of PRA uncertainties on the risk importance measures and their utilization need to be addressed. Even though formal uncertainty analysis can be performed, such an evaluation may not be necessary. Sensitivity analyses could be performed as a substitute for a formal uncertainty evaluation. The following sensitivity analyses are designed to reveal any additional high risk or marginal risk importance that could occur under different plausible assumptions or scenarios which then can be included in the higher class as a precaution against PRA uncertainties.

Component-Specific Sensitivity Analyses

This sensitivity analysis is designed to address the failure rate uncertainty of a component and its potential impact on ranking. For those components that are ranked low, a sensitivity analysis using the 95th percentile of the unavailability distributions of the components could be performed to determine the impact on FV measures. This could be done for each component or human error individually. The unavailability of some components with large uncertainties, such as check valves, could cause them to shift from the low to high categories. If this occurs, the components could be shifted to a higher category to account for the uncertainty distribution.

Sensitivity Analyses for a Component Group

Sensitivity analyses are designed to address the correlated change in a failure rate of a group of components. The sensitivity analyses could also address the correlated changes in the failure rate of a group of components from such causes as aging and wear. For a group of components (e.g., breakers), identify those that are binned in the low category. Increase the mean failure rate of all selected components in a manner consistent with a generic error factor associated with the component type. Identify those components that are shifted to a higher category for further consideration to be removed from the low bin category.

Sensitivity Analysis for 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 generally not modeled in PRAs. Component-level importance measures (e.g., RAW, RRW, and FV) are typically calculated based on assumed nominal values of modeled basic events. Some component importance measures (i.e., FV measure) could 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 HSSC mainly because of its contribution to CCFs, or a component may be ranked as LSSC mainly because it has negligible or no contribution to CCFs. A component may be ranked insignificant either because of omission of CCF contributors or because of the assignment of an insignificant CCF contribution. Thus, removing or relaxing requirements may increase the CCF contribution, thereby changing the ranking order. The following approach ensures that relative ranking of components include proper consideration of the CCF contributions:

- If a component is ranked low because the CCF is not included in the PRA model, revisit the CCF models to ensure that the assumption of no CCF is valid (especially under the potential relaxation of requirements for low risk components).

Set all CCF contributions to zero and rank the components. Special care should be given to truncation limits used in PRA quantification for this case run. Identify components that shift to a higher category. To defend against the uncertainties associated with CCF contribution, these components should be treated as higher-category components.

Sensitivity Analysis for Recovery Actions

PRA's typically model recovery actions especially for dominant accident sequences (but not for all sequences). Quantification of recovery actions typically depends on the time available for diagnosis and performing the action, training, procedures, 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 risk insignificant.

Sensitivity analyses can be used to show how the SSC ranking may change if one removes all recovery actions (setting their failure probability to one). The objective is to determine if a component that was ranked low will move up to a high or medium risk category. If so, the component should be removed from the low category.

A.3 Safety-Based Prioritization

The major objective for safety-based prioritization is to evaluate and identify those areas where proposed regulatory changes may result in potentially undesirable safety degradations which cannot be easily shown with the PRA-based prioritization. This could include those items (SSCs and human actions) that either are not explicitly modeled in PRA or are not within the current scope of the PRA. It also could include those safety concerns that are not captured by the severe accident risk typically modeled in PRA's. Specific areas of safety concerns are defense-in-depth and the plant safety margins. The specific issues to be addressed are discussed below.

Defense-in-Depth

To assure that the philosophy of defense-in-depth is maintained, the following should be examined:

1. Assure reasonable balance among prevention of core damage, prevention of containment failure, and consequence mitigation.

Compliance with decision guidelines for CDF and LERF could assure to a great extent balance between the prevention of core damage and early containment failure. Considerations for emergency planning and potential for late containment failures should also be accounted for to assure that these mitigative features and the associated SSCs are not degraded by the proposed change.

2. Avoid overreliance programmatic activities to compensate for weaknesses in plant design.

There could be instances that meeting the quantitative guidelines for CDF and LERF are strongly dependent on the credit taken for programmatic activities. Overreliance on programmatic activities such as maintenance, surveillance, and recovery actions to compensate for the proposed change should be avoided. The sensitivity analyses on the recovery actions proposed earlier and the data related discussion in the body of this report could be used for addressing this issue.

3. Maintain system redundancy, independence, and diversity.

The qualitative PRA results, i.e., the accident sequence minimal cutsets, show what combinations of passive and active failures would cause core damage or radioactivity release, and thereby reflect directly on the defense-in-depth concept. The minimal cutsets can show the effective redundancy and diversity of the plant design. Qualitative PRA results should be used to demonstrate that system redundancy, independence, and diversity are maintained commensurate with the expected frequency and consequences of challenges to the system.

4. Maintain defense against potential CCF and the avoid introduction of new CCF mechanisms.

Relaxation of programmatic activities could exacerbate an existing CCF mechanism or could introduce new sources of CCFs. Even though the CCF treatment is reserved for CCFs within a system, here we are concerned about the CCFs across systems, i.e., concurrent trends of degrading reliability among a set of components for which requirements are relaxed.

5. Independence of barriers is not compromised.

Generally, the barriers are passive and of such a diverse nature that changes in requirements are unlikely to cause them to fail or degrade dependently. However, there are some failure mechanisms that could be of concern under certain application specific proposals. One such mechanism, which could cause failure of more than one defense-in-depth barrier, is the CCF mechanism. For example, if a new CCF mechanism is introduced for both inboard and outboard isolation valves, then primary coolant rupture outside the containment could bypass the containment. In this case, the potential could exist for failure of two defense-in-depth barriers even though highly unlikely. Identification and proper application specific treatment of such mechanisms capable of failing or degrading multiple barriers should be considered in proposed changes.

6. Defenses against human errors are maintained.

Considerations to avoid overreliance on human actions for protecting the core and the defense-in-depth barriers were discussed earlier. Defenses against human errors which under a change request may become more likely and contribute significantly to risk should also be taken. The proposed changes and its effect on potential human errors should be assessed. Careful attention should be paid to those cases where a proposed change could impact the performance and reliability of those equipment used by the operators to perform the necessary actions, e.g., lighting, communication devices, instrumentation and control devices, and other operator aids, such as alarms and displays.

Safety Margins

To assure adequate safety margins are maintained, the following should be examined:

1. Code and standards or alternatives approved for use by the NRC are met.

Specific considerations outlined in application specific guide should be followed to assure that the proposed changes are not in conflict with NRC approved codes and standards (e.g., ASME standard referred to in 10 CFR Part 50.55a).

2. Safety analysis acceptance criteria in the Final Safety Analysis Report (FSAR) are met

The impact of the proposed changes on the assumptions, initial, and boundary conditions used for FSAR safety analysis should be examined to assure the changes are within the acceptable limits and the existing safety margins are maintained.

There are other qualitative considerations that need to be examined to assure that categorizing a component as a LSSC will not result in an adverse safety impact. There should be at least one set of supporting SSCs that are categorized high and could prevent the occurrence of the initiators and the failure of the supercomponents that are modeled in PRAs. This is one way of assuring that the low frequencies for the initiators and high reliability of supercomponents that are credited in PRAs are maintained specially when they are either of high or medium importance. The examination of the following questions can help the qualitative prioritization of those SSCs not explicitly modeled in PRAs:

1. Can the failure of the SSC result in the eventual occurrence of an initiating event?
2. Can the failure of the SSC result in a failure of a supercomponent that is modeled in the PRA and expected to be either high or medium SSC?
3. Does the SSC belong to a set of redundant components such that they are susceptible to a CCF and their failure could cause eventual failure of a supercomponent or an initiator in PRA which is expected to be either in high or medium categories?
4. Does the SSC belong to a component class in which relaxing the requirements may significantly impact its reliability (e.g., the role of periodic overhaul in circuit breakers)?
5. Can the SSC support operator and recovery actions specially those credited in the PRA?
6. Is the SSC currently included in the scope of current regulatory requirements?
7. Does the SSC play an important role in the post severe accident activities (e.g., monitoring)?

When an SSC is categorized based on qualitative considerations, discussion should be provided on the SSC function, reasons for selecting the category, why it was not modeled in a PRA, and the potential impact of proposed changes if any.

A.4 Integration

Following the earlier discussion, an SSC or a human action may be assigned to a category by a quantitative PRA-based prioritization, a qualitative PRA-based prioritization, or a qualitative safety-based prioritization. An integral list of SSCs and human errors belonging to a given category taking into account these different prioritization methods needs to be constructed for most of the applications. A process for this integration is summarized below.

Combined Quantitative List

Results of the quantitative prioritization using the baseline PRA (based on CDF and LERF) are combined simply by identifying as HSSCs based on either CDF or LERF. Low risk significant list (LSSCs) is comprised of items common to both CDF and LERF. A combined list of the HSSCs and the LSSCs that are covered by the scope of the risk-informed application and are within the scope of PRA then could be constructed.

Combined Qualitative List

Items (SSCs and human actions) within the scope of risk-informed application under consideration and not identified in the combined quantitative list as high risk significant would be the subject for qualitative prioritization. Qualitative ranking (as described in Sections A.2.2 and A.3) would include both the qualitative PRA-based and the qualitative safety-based items. Qualitative ranking is done based on examination of the PRA minimal cutsets, defense-in-depth consideration, safety margin consideration, and general safety consideration, especially for those items that are either not explicitly modeled in the PRA or not within the scope of the PRA. Items examined by different approaches for qualitative ranking that are identified as high safety significant are combined and listed. Contributing factors and the reasons behind this ranking should be documented.

Integrated List

Those items identified as HSSCs (quantitative) and those identified as high safety significance (qualitative) could be combined into a more comprehensive safety significance list. All remaining items within the scope of the application then could be listed in a less safety significance item list. There could be some instances where an additional category such as medium safety significance is defined. The process of integration described here could still be applied.

Use of the Integrated List

The integrated HSSC and LSSC lists could be used to identify the candidates for either risk beneficial changes or potential regulatory relaxations. Compensatory measures could be considered for those items in the integrated more safety significance list since substantial risk reduction could be achieved. Regulatory relaxation could be considered for those items in the integrated LSSC list since major saving in resources could be obtained without degrading safety. The lists of high and low safety significant (HSSC/LSSC) items are expected to be robust and should not change significantly as a result of the proposed changes. However, if post change ranking indicates that some items have shifted from low safety significant to high safety significant list, those items should be considered for performance monitoring and phasing in implementation of changes.

APPENDIX B. PRA PEER REVIEW

An independent peer review is a way of assuring the adequacy of the probabilistic risk assessment (PRA) used in risk-informed regulatory applications and to examine the validity of the risk impact estimated for the proposed changes. This appendix discusses the objectives and scope of an independent peer review and describes an example process for conducting the peer reviews.

B.1 Objectives of the Review

Independent peer reviews are performed to address both the adequacy of the PRA used for a risk-informed regulatory submittal and the validity of the estimated risk impact resulting from the proposed changes. The peer review is a means of assuring technical quality of the PRA and its applications. The subject of peer review is further addressed in NUREG/CR-6372^(B.1). The specific goals of the peer review are:

- to determine the adequacy of the baseline PRA to support one or more types of applications,
- to determine the validity of the input information sources, assumptions, models, data, and analyses forming the basis for the proposed change (or changes), and
- to determine the validity of the results obtained in the analyses and the corresponding conclusions related to the proposed change (or changes).

To provide assurance that the approaches were generally applied appropriately, the peer reviewers should compare the baseline PRA against the attributes listed in this report and perform spot checks on each portion of the baseline PRA and its risk-informed application. The peer reviewer should report those problems that are significant enough to change the conclusion of whether or not a proposed change(s) is risk significant. The peer reviewers should separately note problems that would not change the conclusions for the particular change being proposed but are expected to be significant for other changes that might be proposed in the future.

B.2 Review Team Composition and Qualifications

The peer reviews will normally need to be performed by a team, rather than an individual, because the basic tasks in the analyses generally involve expertise in multiple disciplines. For the PRA peer review and depending on the scope of the baseline PRA, experts may be needed in the following areas: systems analysis, data analysis, human reliability analysis (HRA), severe accident phenomena (if a Level 2 analysis was performed for the submittal), source term (if a Level 2 analysis was performed for the submittal), consequence modeling (if a Level 3 analysis was performed for the submittal), seismic analysis (if part of submittal), fire analysis (if part of submittal), and for analysis of "other" external events as appropriate for the plant site.

Each peer reviewer must have experience with nuclear power plants in performing the PRA task that the reviewer is assigned to review. This experience is expected to include knowledge of typical inputs, assumptions, methods and techniques, models, scope, level of detail, data, and form of results for the assigned review area. The reviewers should be cognizant of the issues addressed in this report and understand the impact of the delineated attributes on the quality

^{B.1}"Senior Seismic Hazard Analysis Committee Report," NUREG/CR-6372, to be published, 1997.

of PRA. The reviewers should also have at least a general familiarity with the plant design being analyzed. At least one member should have a good knowledge of the specific plant and its operation.

B.3 Review Process and Considerations

The peer review proceeds in two phases. In the first phase, the adequacy of the baseline PRA to support the intended applications is determined. In the second phase, the use of the baseline PRA for estimating the risk impact for one or more applications is reviewed. It is more efficient to conduct peer reviews in an interactive manner, especially before the completion of the application. In the second phase review, the peer reviewers could accept a previous peer review team's conclusions for the baseline PRA model but would examine any previously unresolved issues that were documented by the previous peer review team(s) to determine whether they are important for the current application. The peer reviewers also examine any changes made to the baseline PRA to determine the acceptability of the change, and the reasonableness of the results. A meeting of the review team would begin with a discussion of the proposed change, to ensure that the team has a good understanding of the proposed change and its implications.

The two major functions to be performed by the peer reviewers are to determine if the analyses are acceptable, and the results are reasonable. The peer reviewers should substantiate their conclusions. These two peer review functions are applicable for each PRA task and for both of the two review phases.

The first function of the peer review is to examine the inputs, techniques, and analyses for the PRA. In performing the review, attention is given to the completeness and the accuracy of information so that the PRA reflects a realistic picture of the as-built, as-operated plant. The analyses assumptions are based on the use of plant walkdowns, controlled documentation concerning the plant design and operation, involvement of plant staff, and a "freeze date" for the analysis (including any updates). The peer review would examine the analyses inputs to determine that the sources of data are justifiable and traceable.

The second function of the peer review is to verify that the results of the study are reasonable. The peer reviewers compare the results against studies from similar plants. Major differences are identified and rationalized. Selected portions of the study, especially those with significant impact on the conclusions of the study, are selected for independent re-evaluation.

The comments generated by the peer reviewer would be documented and specific recommendations highlighted. The utility response including their commitments regarding potential modifications to the analyses would also be documented for future reviews.

The following provides a summary discussion on the major inputs and outputs to the baseline PRA tasks that are examined by the peer review team. The level of detail for the review should be commensurate with the scope of the applications. A list of example issues and considerations for evaluating the risk impact of the proposed changes on a Level 1 internal event PRA is provided in Table B.1.

Table B.1 Example of issues and considerations for risk impact evaluation of proposed changes

Level 1 (Internal Event PRA)**Initiating Events**

- Does the application introduce potential for 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?

Success Criteria

- Does the application necessitate modification of the success criteria either for support or frontline systems?

Event Trees

- Does the application necessitate the introduction of new branches or top events to represent new concerns not adequately addressed in event trees?
- Does the application affect the dependency among the event tree branches thereby requiring re-ordering of branch points?

System or Component Reliability Models

- Does the application impact system unavailabilities in ways that underestimate the reliability results predicted by the current simplified models?
- Does the application impact the support functions to systems and components in such ways as to alter the dependency in the models?

PRA Data

- Does the application change the conditions and environment under which systems and/or components are demanded such that the current failure rates may need to be changed?
- Does the application changes the failure rates such that the previous plant-specific data may not be adequate?
- Does the application changes the data such that it may require additional test and data analysis effort?

Dependent Failure Analysis

- Does the application introduce the potential for new common-cause failures (CCFs)?
- Could the application changes the CCF component groups already modeled in the PRA?
- Could the application affect the CCF probabilities? How is this addressed?

Human Reliability Analysis

- Does the application involve procedure changes?
- Could the application introduce new human error potentials?
- Does the application change the available time for human actions?
- Does the application affect the recovery actions?

Appendix B PRA Peer Review

Level 1 Modeling

The items to be examined for the overall examination are discussed first. The documentation that should be furnished to the review team is discussed in Chapter 3 of DG-1061^(B.2) and throughout various chapters in this report. The items for review for the overall examination are:

- The initiating events included in the PRA are reviewed to assess the completeness of the initiators considered, to assess whether the basis for excluding any initiators is adequate, to check for new initiators introduced by the proposed change(s), and to determine the reasonableness of the initiator frequencies used in the PRA.
- The reviewers consider whether the success criteria for each initiator is reasonable, check the impact of proposed changes in these criteria, and determine if there is an adequate basis for any success criteria that is not typical for the type of plant being reviewed.
- The accident sequence models are examined to determine whether the plant response to the initiators are appropriately accounted for in the event trees.
- The modeling of systems is reviewed to determine whether the failures considered are comprehensive. Operability during accident and harsh environments (e.g., trip points for reactor core isolation cooling system) would be considered as well as the completeness of the failure modes (e.g., failure to start, run), including common-cause failures and human errors.
- The system dependency matrix is reviewed to assess whether dependencies are appropriately considered in the PRA.
- The operator actions that are included in the PRA, the failure probabilities for the actions, and the basis for excluding actions from the analysis are reviewed to determine the completeness of the analysis and the reasonableness of the probabilities estimated for each operator action (in the baseline and post change case).
- While the peer review is not expected to provide a detailed review of all failure frequencies/probabilities used in the PRA, the methods used for determining the failure frequencies/probabilities (including common-cause treatment) are examined. The adequacy of data sources are also assessed together with the failure frequencies/probabilities (including common-cause values), and the associated uncertainties.
- The adequacy of the quantification method, including the screening criteria, cutset truncation level, and use of recovery actions are addressed.
- The development of plant operating states (POS) and the calculated fraction of time in each POS is reviewed if the PRA includes a low power/shutdown evaluation.

^{B.2}USNRC, "An approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis," Draft Regulatory Guide DG-1061, February 1997.

If a fire analysis is included in the PRA, the following is examined:

- development of fire areas/zones, including the basis for screening,
- adequacy of cable tracing, including adequacy of justification provided by utility for any cables not traced,
- adequacy of damage modes considered in the analysis,
- adequacy of fire propagation analysis, including treatment of fire suppression and barrier failure probabilities, and
- adequacy of HRA models.

- If a seismic analysis is included in the PRA, the adequacy of the seismic hazard curve used in the PRA is reviewed. The reviewers also examine the approach used to calculate component fragilities and the calculated fragilities for reasonableness.

To supplement the items listed above, the independent peer reviewers also perform detailed spot checks of selected accident sequence models (e.g., event trees), systems models (e.g., fault trees), and the associated quantification. The reviewers are also expected to spot check the documentation of plant walkdowns (done for any operating mode and for internal or external events).

Level 2/3 Modeling

The review needed for the Level 2/3 analysis will depend on the approach used by the licensee. If the licensee chooses to use the simplified approach described in Appendix B of DG-1061, then the review will only need to consider the approach used to map the Level 1 results into the simplified event trees (unless the peer review team judges the DG-1061 Appendix B partitioning factors to be inadequate). If a full Level 2/3 analysis is performed, the review team will need to evaluate the adequacy of the Level 2/3 analyses relative to the attributes described in this NUREG report.

If the simplified Level 2/3 treatment is used, the following would be checked:

- Examine the criteria used to group the Level 1 cutsets into categories for calculating the split fractions for the system response branches in the simplified event trees to assess whether or not the Level 1 results are appropriately characterized for the Level 2 results.
- Review the approach used to calculate the split fractions to ensure they are calculated correctly and examine the calculated split fractions to determine whether they appear reasonable.

If a full Level 2/3 analysis is performed, the following would be checked against the attributes provided in this report:

- Examine the criteria used to group the Level 1 cutsets into appropriate plant damage states.
- The event trees (or equivalent system models) are reviewed to determine whether the treatment of severe accident phenomena is comprehensive for the plant under consideration. The treatment of systems and phenomena are reviewed, including the basis for probabilities, to determine if they are consistent with the attributes provided in this report.
- The containment failure modes and the associated probabilities are reviewed to verify they are reasonable.

Appendix B PRA Peer Review

- The source term and consequence modeling and inputs are reviewed to determine whether they are consistent with the attributes provided in this document.
- The process used to bin results for the Level 2/3 analysis are checked (e.g., plant damage states, accident progression bins, or source term groups) to ensure that the grouping maintains the separate effects of the key factors affecting the results. The actual mechanics of the binning are examined for selected cases to determine whether the calculations were performed correctly.

Review of PRA Results

In addition to reviewing the inputs to the PRA, the peer review team would also provide an independent evaluation of the sensibility of the results. The review would focus on the appropriateness of the identified dominant accident sequences, and when a full Level 2/3 analysis is performed, the containment failure modes, releases and consequences. The review would also consider whether the aspects of the plant design, operation, and maintenance that are found to contribute most to risk in the PRA are reasonable. The results examined are:

- The top cutsets are scanned, looking for unreasonable combinations of events.
- The sequence level contributions to CDF calculated before and after crediting recovery actions are scanned for reasonableness.
- The total plant CDF (including uncertainty) calculated before and after the proposed change are assessed for reasonableness.
- The frequencies for the early containment failure and containment bypass are reviewed for reasonableness if the utility is performing a simplified Level 2 analysis. The frequencies of accident progression pathways as grouped for source term calculations, the frequencies and magnitudes of source terms, the individual early and latent fatality frequencies, and the uncertainty characterizations for these frequencies are assessed for reasonableness if the utility is performing a full Level 2/3 PRA.

B.4 Documentation of Findings

The documentation should include descriptions of the peer review process and findings and the utility responses to the peer review findings. For the peer review of a baseline PRA, the adequacy of the individual PRA tasks as compared to the attributes of an acceptable PRA should be documented. Any weaknesses of the PRA should be clearly identified. For a particular application of the PRA, the appropriateness of the PRA manipulation should be documented especially with regards to identified weaknesses in the baseline PRA. The documentation of findings should be included with the submittal of the proposed change to the NRC.

GLOSSARY

Accident analysis — steps taken by a PRA analyst to model and quantify the frequency of core damage, containment response, and public risk attributable to a specific accident or class of accidents

Accident conditions — environmental or operational conditions occurring during events that are not expected in the course of plant operation but are postulated for design or analysis purposes

Accident initiators — initiating events that can challenge plant systems and components

Accident progression analysis — modeling of that part of the accident sequence which follows the onset of core damage, including containment response to severe accident conditions, equipment availability, and operator performance (also referred to as a Level 2 PRA)

Accident sequence analysis — the process of determining the combinations of initiating events, safety functions, and system failures and successes that may lead to core damage (also referred to as a Level 1 PRA)

As-built, as-operated — a phrase used to refer to the conformity of the PRA model to the actual operational and design conditions at the nuclear plant

Availability — the probability that a system or component will function satisfactorily when required to respond to a randomly occurring initiating event or system/component challenge (unavailability is the complement of availability)

Best estimate — the point estimate of a parameter used in a computation which is not biased by conservatism or optimism

Burden — in human reliability analysis, any of the factors that affect operator performance including such items as time constraints (short available time), diagnosis constraints (confusing indications), factors related to decisionmaking (competing resources), command and control impediments (remoteness between people who need to communicate), and physiological factors (hostile environment)

Common cause event — a subset of dependent events in which two or more component fault states exist at the same time, or within a short time interval, and are the direct result of a shared cause

Common cause failure — a single event that adversely affects two or more components at the same time

Component — an element of plant hardware designed to provide a particular function (for system modeling purposes, a component is at the lowest level of detail in the representation of plant hardware in the models)

Conditional containment failure probability — the likelihood, expressed as a probability, that the containment will fail, given that core damage has occurred

Conditional probability — the conditional probability of event A occurring given that event B has already occurred is given as: $P(A|B) = P(A \cap B)/P(B)$

Glossary

Containment bypass — an event which opens a flow path that allows the release of radioactive material directly to the environment bypassing the containment atmosphere

Containment failure — loss of integrity of the containment pressure boundary (caused by severe accident conditions) which results in leak rates to the environment that exceed the design limits

Containment failure mechanisms — accident conditions that can cause loss of containment integrity (examples for severe accidents include failures resulting from direct containment heating, steam explosions [in-vessel and ex-vessel], hydrogen combustion/detonation and shell melt-through)

Containment failure modes — descriptions used to classify the type of containment failure, such as isolation failure, bypass failure, and early or late failure

Containment isolation failure — failure to isolate all lines that penetrate the containment (the frequency of containment isolation failure includes the frequency of pre-existing unisolable leaks)

Containment performance — a measure of the response of nuclear plant containments to severe accident challenges (containment performance is typically represented by the conditional containment failure probability)

Core-concrete interaction - interaction of molten core material with concrete structures in the containment during a severe accident in which the reactor pressure vessel fails

Core damage — uncover and heatup of the reactor core as a result of a loss of core cooling to the point where prolonged clad oxidation and fuel damage is anticipated

Core damage frequency — the frequency, per reactor year, of an accident leading to core damage

Core melt — severe damage to the reactor fuel and core internal structures following the onset of core damage, including the melting and relocation of core materials

Creep rupture - a mechanism of failure resulting from continuous deformation at constant stress; important for metal components at elevated temperatures, such as steam generator tubes or a steel containment boundary in contact with molten core material

Cutset — minimum combination of a set of events (e.g., initiating event and component failures) that, if they occur, will result in the onset of core damage

Dependency — requirement external to an item and upon which its function depends

Diagnosis — examination and evaluation of data to determine either the condition of a structure, system, or component, or the cause of the condition

Dominant contributor — an accident class that has a major impact on the total core damage frequency or a containment failure mechanism having a major impact on the total radionuclide release frequency

Early containment failure — failure of the containment system that occurs early (i.e., relative to the overall timing of the severe accident (typically, early containment failure is defined as containment failure before or within a few hours of reactor vessel breach)

Early release — a radioactive release from the containment that occurs early (i.e., occurring within a few hours of vessel breach) and typically before effective implementation of the offsite emergency response and protective actions

Equipment qualification — the generation and maintenance of data and documentation to ensure that the equipment will operate on demand to meet system performance requirements during design basis accidents

Event tree — a quantifiable logical network that begins with an accident initiator or condition and progresses through a series of branches that represent possible system performance, human actions, or phenomena that yield either a safe, stable state or an undesirable one, such as core damage or containment failure

Event tree top event — the conditions (system behavior or operability, human actions, or phenomenological events) that are considered at each branch point in an event tree

External event — an event initiated outside the plant systems that can affect the operability of plant systems (examples include earthquakes, tornados, and floods and fires from sources outside the plant)

Failure — a state that renders a component incapable of performing its specified operation according to established success criteria (the component can fail if it either functions when not required, or does not function when required)

Failure analysis — the systematic process of determining and documenting the mode, mechanism, causes, and root cause of failure of a component or system

Failure mechanism — any of the processes that result in failure, including chemical, electrical, mechanical, physical, thermal, and human factors

Failure mode — manner or state in which a system or component fails (examples include stuck-open valves, motor-bearing seizure, excessive leakage, and failure to produce a signal that drops control rods)

Failure rate — the number of failures of an item within the population per unit measure of life in such terms as demand or time

Fault tree — a graphical representation showing the logical relationships among faults; provides a concise and orderly description of the various combinations of possible fault events within a system which could result in some predefined, undesirable event for the system

Fault tree analysis — analysis based on probabilities, and mathematical manipulation of those probabilities. (Fault tree analysis begins with an undesired top event and attempts to identify the sub-events that are necessary to cause the top event; fault tree analysis contrasts with failure modes and effects analysis, which is a bottom-up approach)

Freeze date — the cut-off date for the plant model in an individual plant examination; plant modifications after this date are not included in the model

Glossary

Frequency f — the number of occurrences of an event per unit time

Frontline systems — an engineered safety system used to provide core or containment cooling and to prevent core damage or containment failure (such as emergency core cooling and containment spray systems)

Fuel-coolant interaction — the energetic interaction, by direct contact between water and molten core material, that may result in a steam explosion (fuel-coolant interactions may occur either in-vessel or ex-vessel)

Fussell-Vesely importance — the fractional decrease in total core damage frequency when the plant feature (e.g., a component, train, or system) is assumed to be perfectly reliable (failure rate = 0.0)

Generic failure rate — failure rates that apply generically to a class of equipment rather than specifically to an individual piece of equipment. (Rates for equipment from a specific vendor or for a specific application may vary from generic values. Generic failure rates, also called "handbook" failure rates, are useful in preliminary design analysis, predictions, and design planning to estimate inherent capability but should not be preferred to more specific, actual component data, if available.)

Harsh environment — an environment expected as a result of the postulated accident conditions appropriate for the design basis or beyond-design basis accidents

High pressure melt ejection — a reactor vessel failure mode that occurs with the reactor coolant system at high pressure and results in rapid dispersal of molten core material, steam, and hydrogen into the containment, challenging it in two ways:

- (1) The high temperature core material may come in contact with the containment liner resulting in liner failure
- (2) The dispersal of core material and steam into the containment atmosphere may result in direct containment heating and, possibly, hydrogen combustion

Human error probability — a measure of the likelihood that the operator will fail to initiate the correct, required, or specified action or response needed to allow the continuous or correct function of an item of equipment

Human reliability analysis — a structured approach used to identify potential human errors and to systematically estimate the probability of those errors using data, models, or expert judgement

Individual plant examination - Generic letter 88-20 requested U.S. nuclear utilities to perform an evaluation to identify any plant-specific vulnerabilities to severe accidents. In responding to GL 88-20 most utilities performed the equivalent of a Level 2 PRA, and considered accidents initiated by internal events during full power operation

Initiating event - see accident initiators

Internal events — accident initiators originating in a nuclear power plant and, in combination with safety system failures and/or operator errors, leading to core damage accident sequences (see also external events)

Late containment failure — failure of the containment in a time considered long relative to the overall timing of the severe accident (typically, late containment failure is defined as containment failure occurring more than a few hours past reactor vessel breach)

Late release - a radioactive release from the containment that occurs late (i.e., occurring more than a few hours past reactor vessel breach) and typically after effective implementation of the offsite emergency response and protective actions

Level 1 analysis — an identification and quantification of the sequences of events leading to the onset of core damage

Level 2 analysis — evaluation of containment response to severe accident challenges and quantification of the mechanisms, amounts, and probabilities of subsequent radioactive material releases from the containment

Level 3 analysis — evaluation and quantification of the resulting consequences to both the public and environment

Level of detail — different levels of logic modeling used in a PRA. (A failure event in a fault tree analysis can address various levels of detail, depending on how much useful information is available concerning the contributors to the failure event)

Low contributor — an accident class that has a minor impact (on the order of a few percent) on the total core damage frequency or a containment failure mechanism having a minor impact on the total radionuclide frequency

Mission time — the time period that a system or component is required to be operable in order to carry out its mission. (For example, a mission time of 24 hours implies that containment sprays are required to be operable for 24 hours in order to prevent containment failure from occurring within that period)

Model — an approximate mathematical representation that simulates the behavior of a process, item, or concept (such as failure rate). (For example, the probability of a system failure is synthesized using models that relate system failures to component failures and human errors. The probability of system failure is then calculated from these more elementary and better understood failures. These models contain parameters, such as the rates of occurrence of various events, that are not known precisely.)

Modeling assumption — an assumption on which a model is based (such assumptions may not be valid or universally accepted)

Plant — a general term used to refer to a nuclear power facility (For example, plant could be used to refer to a single unit or a multi-unit site)

Plant damage state — a set of accident sequences from the Level 1 analysis grouped together because their characteristics relevant to the subsequent progression are similar. The Plant Damage States constitute the interface between the Level 1 and Level 2 analysis of a PRA.

Probabilistic Risk Assessment/Analysis - of a nuclear power plant, is an analytical process that quantifies the potential risk associated with the design, operation, and maintenance of a plant to the health and safety of the public. The risk evaluation involves three sequential parts or "Levels" (refer to Level 1 analysis, Level 2 analysis and Level 3 analysis)

Glossary

Reactor year — a period of the reactor operation that accounts for the downtime during a calendar year

Recovery action — an operator action intended to bring failed equipment back to operable status

Release class — a set of accident progression sequences grouped together because they lead to similar radionuclide releases and for which a single representative release calculation can be performed

Release fraction — the fraction of the total inventory of a radionuclide in the reactor core at the start of the accident which is released to the environment

Reliability — the probability that a component performs its specified function and does not fail under given operating conditions for a prescribed time

Risk — typically, the expected value of the consequences per unit time (usually expressed as fatalities/yr or \$/yr); defined more broadly using the "set of triplets" $\{(s_i, f_i, x_i)\}$. (In the set of triplets, s_i identifies one of several possible scenarios, f_i is the frequency of that scenario, and x_i is the consequence of that scenario. The risk is the set of all possible scenarios, their frequencies, and their consequences. This definition distinguishes between low-frequency, high-consequence scenarios and high-frequency, low-consequence scenarios.)

Risk-informed regulation — a regulation whose decisionmaking criteria integrate probabilistic and conventional deterministic evaluations

Scope — refers to the extent of initiating events considered in a PRA. A full-scope PRA usually includes accidents initiated by internal and external events during full power and low power & shutdown conditions. The scope should be distinguished from the PRA Level, which defines the extent of the analysis (refer to Level 1 analysis, Level 2 analysis and Level 3 analysis).

Sensitivity analysis — an analysis in which one or more input parameters to a model are varied in order to observe their effects on the model predictions

Severe accident — an accident that goes beyond the design-basis of the plant and usually involves extensive core damage

State-of-the-art in PRA — a PRA that reflects the latest improvements in PRA modeling and evaluation

Station blackout — an accident sequence initiated by loss of all offsite power with failure of onsite emergency AC power (diesel generators), and failure of timely recovery of offsite power and onsite emergency AC power

Success criteria — the systems/components and their combinations that are needed to carry out their mission given an accident initiator

Support system — a system that provides a support function (e.g., electric power, control power, and cooling) for another system. (For example, HVAC is often considered as a support system.)

Unavailability — see availability

Uncertainty Analysis — the quantification of the imprecision in the PRA estimate that results from imprecisely formulated PRA models and imprecisely known input variables

Unit — refers to a single nuclear power reactor with its associated systems and components. Most nuclear power plant sites have either one or more units. At multi-unit sites, some support systems can be shared between units

Vessel breach — refers to the failure of the reactor pressure vessel (RPV) boundary and a release of the radioactive material from the RPV

CRGR Main Emphasis March 18, 1997

The Committee to Review Generic Requirements (CRGR) commented on the extensive inter-office cooperative effort which was evident in the development of the general and the application-specific regulatory guides and the associated Standard Review Plans. The Committee commended the various office staff that had demonstrated a well-coordinated concerted effort in developing the extensive guidance for the industry and the staff on a complex subject within the realm of the PRA Implementation Plan for risk-informed regulation.

During the meetings, the CRGR made extensive comments on the specific documents to make an overall improvement in these documents. Broadly speaking, the Committee made the following general observations:

1. Fundamental Approach

The CRGR observed that these documents represented a measured step along the path towards risk-informed regulation. The CRGR recognizes that the allowable increases in risk are small. Thus, the approach proposed is essentially risk neutral within the error bands involved. This is especially relevant in that based on IPE submittals a number of reactors already exceed the subsidiary core damage frequency objective of $1E-4$.

2. Backfit Situation

The CRGR has the responsibility to review and recommend to the EDO approval or disapproval of requirements of staff positions to be imposed by the NRC staff on one or more classes of power reactors. It is the CRGR's understanding that these Regulatory Guides and the accompanying Standard Review Plans are not being imposed (i.e., there is no intent to backfit these provisions). With the understanding that indeed the risk-informed decision process is voluntary, and that viable alternates or approaches remain available to the regulated industry, the CRGR has no objection to these documents going forward.

The CRGR did not review any application or justification under 50.109, as none was tendered to us.

3. Value-Added Role

The Commission has encouraged the CRGR to continue to exercise a value-added role (that is, above and beyond its strict Charter role) in its review. Accordingly, the CRGR offers the following opinions:

a. Use of Small Numbers

The CRGR observed that, in some applications of the general regulatory guide there would be utilization of small numbers, in the PSA space. For example, if a plant had a core damage frequency (CDF) in the vicinity of $1\text{E-4}/\text{yr}$, there could be a limiting increase in CDF in the range of 1E-5 to 1E-6 . Under the proposed new guidance, an increase in CDF would be limited to 1E-6 under normal conditions; or, with increased technical and management review, an increase of 1E-5 might be permitted. In the limiting case, therefore, (i.e., in the near vicinity of $\text{CDF} = 1\text{E-4}$) CDF could increase from 9.8 to $9.9 \times \text{E-5}$ without special management consideration; or, with increased technical and management review, CDF might be permitted to increase from 8.9 to $9.9 \times \text{E-5}$. The Committee agrees with other experts that there is "difficulty in identifying very low frequency initiators in the range of 1E-6 per year or lower."

The Committee further notes that even with the small changes in absolute value of risk, the changes that could be made to the current licensing basis of a plant may be quite significant from an economic viewpoint. However, the Committee cautions on risk ranking schemes that may be used to evaluate the risk significance of systems and/or components - one should not base decisions on the relative order of very low probability sequences.

b. Safety Goals

DG-1061 identifies the role of the Commission's Safety Goal Policy. In particular the guide states that the acceptance guidelines defined "are consistent with the Safety Goals and their subsidiary objectives and changes to the CLB are expected to result in changes in risk which do not exceed the goals and which are no more than a small fraction of these goals and objectives."

c. Monitoring Program

Although the Committee recognizes that monitoring is an important aspect of a performance-based risk-informed regulation approach, care should be taken not to specify the elements of a monitoring program so prescriptively. In that regard, in the proposed guidance documents the staff should consider simplifying the guidance provided on monitoring.