January 12, 2000 SECY-00-0007

FOR: The Commissioners

FROM: William D. Travers /RA/
Executive Director for Operations

SUBJECT: PROPOSED STAFF PLAN FOR LOW POWER AND SHUTDOWN RISK ANALYSIS RESEARCH TO SUPPORT RISK-INFORMED REGULATORY DECISION MAKING

PURPOSE:

To describe the results of studies done to date and request Commission approval for the staff's plans and recommendations for developing guidance, methods, and tools needed to better reflect low power and shutdown risks in risk-informed regulatory decision making.

BACKGROUND:

Both nuclear power plant operational experience and probabilistic risk assessments (PRAs) indicate that the risk associated with low power and shutdown (LPSD) operations could be significant. In the past ten years important events have occurred and a number of NRC, industry, and international studies have concluded that significant frequencies of reactor core damage could occur from accidents initiated during low power and shutdown (LPSD) operations. This perspective has led to several initiatives to ensure safety during such operations, including:

- Reactor licensees have developed and applied methods for better managing plant safety during outages.

- The American Nuclear Society (ANS) has initiated work to develop standards for qualitative and quantitative methods for assessing LPSD risk.

- The NRC has issued generic letters and information notices and performed supporting risk studies with respect to LPSD conditions.

CONTACT:
Mark Cunningham, RES
415-6189

The staff’s work to expand the use of risk assessment, as directed in the Commission’s PRA Policy Statement, brought with it the need to address low power and shutdown accident risks in risk-informed regulatory activities. Regulatory Guide 1.174 provides general guidance with respect to LPSD risks, indicating in Section 2.2.3.1 that:

> [T]he assessment of the risk implications in light of the acceptance guidelines . . . requires that all plant operating modes and initiating events be addressed, [however] it is not necessary to have a PRA that treats all these modes and initiating events. A qualitative treatment of the missing modes and initiators may be sufficient in many cases.

The staff's new reactor oversight program addresses plant performance during LPSD as well as during full power operations. The aim of the program is to focus NRC attention on performance issues that are risk significant. The staff is currently extending the significance determination process, developed to assess the risk significance of inspection findings during full power operations, to cover the low power and shutdown modes. Insights from existing LPSD PRAs are used in the development of this process. At present it is intended to be a conservative screening approach. However, during its implementation phase, if a more realistic risk significance determination process proves to be more appropriate or if licensees apply more detailed models than those currently adopted, more detailed PRA models would need to be incorporated in the process.

The staff’s proposed work to risk-inform 10 CFR Part 50, described in SECY-99-256 and SECY-99-264, also reflects the need to consider LPSD risk. For example, in the Advanced Notice of Proposed Rulemaking attached to SECY-99-256, the staff discusses the PRA scope needed for the proposed Appendix T categorization process. In this discussion (on page 25), the staff indicates that “when categorizing SSCs, the licensee shall also consider . . . shutdown and low power modes of operation, either by PRA modeling or by the integrated decision-making process.”

The staff routinely assesses the significance of operational events, including those occurring during LPSD conditions. The staff uses tools including the “simplified plant analysis risk” (SPAR) models to study such events. The SPAR models are now being extended to incorporate models for LPSD conditions.

While the nuclear industry’s outage management programs, the ANS’s standards development work, and the staff’s risk-informed regulation initiatives reflect the need to consider LPSD risk, there remain concerns that the available methods and tools for estimating this risk are less mature than those for assessing the risks of accidents initiating during full power operations. The Advisory Committee on Reactor Safeguards (ACRS) in its letter to the Commission (from R. L. Seale to Chairman Jackson, April 18, 1997) expressed concerns that the NRC staff did not have an adequate technical understanding of LPSD conditions for rendering timely regulatory decisions of licensee submittals. In follow-on staff discussions with the ACRS, the Committee identified concerns that the staff was not well prepared to provide timely implementation of Regulatory Guide 1.174. The ACRS recommended that the necessary benchmarking of risk during LPSD operations should be established to enable the staff to render timely licensing decisions and guidance for operating plants.

In light of the numerous places in the staff's risk-informed activities in which LPSD risks must be considered, as well as the concerns raised by the ACRS and others, the Commission approved, as part of the FY 1999 budget, additional risk studies associated with low power and shutdown operation. However, as stated in a March 19, 1998, staff requirements memorandum the Commission did not approve staff-recommended work to develop additional shutdown risk acceptance guidelines beyond those in Regulatory Guide 1.174 but rather requested that the results of the additional risk studies be provided for Commission consideration. Accordingly, the attached report and recommendations are being provided to the Commission for approval.[1]

The results of the program's first phase and the proposed plans for the second phase are summarized in this paper and discussed in more detail in the attachment.

DISCUSSION:

In the first phase of its program, the staff has performed a number of tasks, including:

- Gathering information on domestic and international LPSD risk assessment methods and results;
- Meeting with stakeholders to discuss LPSD PRA results, current methods used by licensees to manage LPSD risk, and potential guidance, methods, and tool development needs;
- Evaluating strengths and limitations of available methods and tools for use in regulatory applications;
- Identifying and prioritizing tasks (for the program's second phase) to address identified limitations; and
- Developing a multi-year plan for performing these second-phase tasks.

The results of the first phase are documented in the attached staff report. Briefly, the results show that:

> There remains a broad consensus that the frequencies of core damage accidents initiated during LPSD operations can be significant. Domestic (NRC and industry) and international studies reviewed by the staff, as well as comments provided by stakeholders in public meetings, consistently identify potential accidents initiated during some portions of low power and shutdown operations as significant contributors to the total core damage frequency from licensed nuclear power plants.

[1] An interim status report on this program was provided to the Commission in a June 18, 1999, memorandum from the EDO.

Numerous events that are potentially risk-significant have occurred at U.S. plants during LPSD conditions. These events have required mitigation with plant safety systems to prevent core damage. These events combined with the plant response provide relatively high estimated conditional core damage probabilities (1E-4 to 1E-3) and therefore, from a risk perspective, warrant consideration. In other words, initiating events unique to LPSD suggest the contribution to risk during LPSD from the design and operation of the plant is significant.

Licensees have developed qualitative and quantitative methods and tools for managing safety during LPSD operations. To manage LPSD risk, industry guidance has been developed and implemented which provides a qualitative means for licensees to manage safety during outages. Also, over one-half of the licensees supplement this qualitative guidance with some type of quantitative probabilistic risk analysis tools and information.

Current methods provide a strong foundation for considering LPSD accident risks in regulatory activities. The qualitative and quantitative methods now used by licensees appear to have been very successful in maintaining safety during outages. However, these methods need to be supplemented to permit their use in regulatory applications such as risk-informed license/requirement changes and oversight.

There is a strong need to develop better guidance for licensees and NRC staff on how to use current LPSD risk analysis methods in risk-informed regulatory activities. The staff believes that many of the limitations of current methods could be overcome through the development of guidance. This guidance would address technical issues such as how current qualitative or quantitative methods should be adapted for LPSD risk analysis as well as regulatory process issues such as how such methods can be used in specific risk-informed regulatory activities. The American Nuclear Society's work to develop LPSD risk standards plays a key role in the development of such guidance.

In selected areas there is also a need to improve methods and tools for assessing LPSD accident risk. The staff's evaluation of documented LPSD risk studies, and comments provided by stakeholders, reveal several areas in which methods and tools should be developed or improved for use in risk-informed regulatory decision making. In particular, there appears to be a broad consensus that improvements are needed in human reliability analysis (HRA), radioactive material release and transport (PRA level 2) analysis, and in the analysis of transition periods during low power and shutdown operations (assessing the risk associated with the numerous hardware configuration changes and human actions performed in transitioning the plant configuration to a different state).

The proposed second phase of the staff's program to provide a sound technical basis for addressing LPSD risks in regulatory decision making has four parts:

(1) The staff will actively participate in the ANS's work to develop LPSD PRA standards. ANS has formed a consensus committee (the Risk-Informed Steering Committee (RISC)) whose members are from nuclear licensees, NRC, national laboratories, consulting engineering firms, vendors, and academia. A small writing team, reporting to this steering committee, composed of PRA experts in LPSD has also been formed. It is

the intent of ANS to develop a standard for both a plant-specific LPSD PRA and a (qualitative) non-PRA approach which could be used in risk-informed decision making. ANS plans to issue a draft standard for public review and comment in September 2000 and final version in June 2001. The staff anticipates providing support in the resolution of technical issues.

(2) The staff proposes to develop improved guidance for considering LPSD risks. This guidance would be developed for risk-informed licensing decisions (by, for example, supplementing the acceptance guidelines in Regulatory Guide 1.174 to specifically address LPSD risk as previously proposed in SECY-97-287 and Standard Review Plan Chapter 19 to specifically address guidelines for review of LPSD risk analysis), and would be utilized in developing proposed revisions to 10 CFR 50. This work would be performed in FY 2000 and early FY 2001.

(3) The staff proposes to develop improved methods and tools for assessing HRA and Level 2 risk. These areas merit different consideration under LPSD conditions than how they are treated in full-power operation. In addition, a better understanding of these areas is needed because of the large uncertainties associated with them and because of their potential to directly impact staff risk-informed regulatory activities. This work would be performed in FY 2000 and FY 2001.

(4) The staff proposes to evaluate areas identified by the ACRS and other stakeholders as potentially important to risk. Development of improved methods or tools for these areas would be to the extent necessary to address the specific technical issue. To the extent possible and appropriate, this work would be performed in cooperative programs with the nuclear industry and NRC's international PRA research partners.[2] Example areas include transition risk, drain-down events. This work would be performed in FY 2000 and FY 2001; however, depending on the complexity of the work, this effort may extend beyond FY 2001. Any resource needs beyond FY 2001 will be included in the FY 2002 budget formulation process.

RESOURCES:

The staff has estimated that the four parts of the proposed second phase would require the following resources:

[2] NRC's International Cooperative PRA Research (COOPRA) Program, initiated in 1997 to identify and perform cooperative research, has a working group on LPSD risk assessment. PRA experts from fifteen countries participate in this working group.

TASKS		FY 2000	FY 2001
1. Support development of ANS LPSD PRA standard:	Total ($k) FTE	200 0.5	100 0.5
2. Develop improved guidance:	Total ($k) FTE	100 0.5	100 0.5
3. Improved methods and guidance: note (a)	Total ($k) FTE	150 0.5	250 1.5
4. Evaluate potentially important areas: (b)	Total ($k) FTE	100 0.5	500 1

(a) The HRA work is scheduled and costed as part of the HRA research program.
(b) The cost assumes that simple methods and tools can be used in the evaluation and, if necessary, developed; however, if more detailed analysis or development is needed, this effort is not included in the cost estimate.

FY2000 resources shown in this table are included in the current RES budget for LPSD and Part 50. Consistent with Commission guidance, FY2001 resources are not included in the agency's budget, as described in the Fiscal Year 2001 Budget Estimates and Performance Plan (Blue Book). Pending a Commission SRM on these recommendations, reprogramming to accommodate additional funding requirements in FY 2001 and resource requirements for FY 2002 will be addressed in the agency's FY 2002 budget formulation process.

COORDINATION:

The Office of the Chief Financial Officer has reviewed this paper for resource implications and has no objections.

The topic of low power and shutdown risk has been the subject of continuing interactions between the staff and ACRS. The staff briefed the ACRS on a draft version of the attached report on November 18 and December 2, 1999, and modified the report to reflect comments received. The Committee will continue its consideration of the staff's plans using the final version of this paper, as provided to the Commission. A formal letter from ACRS on the staff's plans is expected in February 2000.

RECOMMENDATION:

The staff recommends that the Commission approve the proposed LPSD research plan as described in the attachment.

William D. Travers
Executive Director
for Operations

Attachment:
Perspectives Report on Low Power and Shutdown Risk

LOW POWER AND SHUTDOWN RISK: A PERSPECTIVES REPORT

Prepared by:
Probabilistic Risk Analysis Branch
Division of Risk Analysis and Applications
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

December 1999

TABLE OF CONTENTS

TABLE OF CONTENTS (cont'd)

Section Page

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1 Background

Both nuclear power plant operational experience and probabilistic risk assessments (PRAs) indicate that the risk associated with low power and shutdown (LPSD) operations could be significant. With respect to the former, some important events are: the loss of residual heat removal (RHR) at Diablo Canyon (1987), the loss of AC power and RHR during mid-loop operations at Vogtle (1990), the draindown event at Wolf Creek (1994), and the flooding of the emergency core cooling system at Washington Nuclear Plant - Unit 2 (1998).

With respect to LPSD risk, the NRC performed two PRAs, one for a boiling water reactor (BWR) (Grand Gulf Unit 1, Ref 1.1) and one for a pressurized water reactor (PWR) (Surry Unit 1, Ref 1.2). Several utilities have also performed LPSD PRAs and significant efforts have been devoted to develop software tools for performing LPSD risk assessments and applying these and more qualitative tools to manage risk during outages.

The occurrence of such events resulted in an increased NRC and industry focus on LPSD operations. The NRC undertook many initiatives to improve its oversight of LPSD operations. Examples are the assessments of the Diablo Canyon event (Ref. 1.3) and of the Vogtle event (Ref.1.4), the issuance of the Generic Letter 88-17, "Loss of Decay Heat Removal," the proposed rule for shutdown and fuel storage pool operation (Ref. 1.5), and the Commission's direction on "The Use of Industry Voluntary Initiatives in the Regulatory Process," (Ref. 1.6). On the industry side, the Nuclear Management and Resources Council (NUMARC) developed guidelines for the industry to assess shutdown management (NUMARC 91-06, Ref. 1.7) which were adopted and implemented by the utilities.

At the same time, significant efforts have been undertaken on using quantitative risk information in the NRC's decision-making processes (risk-informed regulation). The Commission published its PRA Policy Statement (Ref 1.8) encouraging the use PRA and the expansion of " the scope of PRA applications in all nuclear regulatory matters to the extent supported by the state-of-the-art in terms of methods and data."

Since the publication of the PRA Policy Statement, the staff has published Regulatory Guide (RG) 1.174, which provides guidance for the use of risk information in regulatory decision-making and has embarked into the use of risk information in all different aspects of regulation, including inspection and enforcement, performance evaluation and monitoring, and risk-informing 10 CFR Part 50. Therefore, the importance for the NRC having the capability to incorporate the risk associated with LPSD operations into risk-informed regulatory activities has increased.

Although all nuclear power plants have done a PRA for the reactor at full power as part of the Individual Plant Examination Program (Generic Letter 88-20), few plants have done a PRA for the reactor in low-power or shutdown conditions. As noted above, the NRC's efforts for quantifying LPSD risk has been limited to two PRAs and to the risk assessment calculations performed as part of the LPSD rule-making activities.

The Advisory Committee on Reactor Safeguards (ACRS) (Ref 1.9) expressed concerns that the NRC staff did not have an adequate understanding of the risk associated with LPSD conditions for rendering timely regulatory decisions of licensee submittals and, in follow-on discussions, recommended that the necessary benchmarking of risk during LPSD operations should be established. The staff, as part of the NRC budget for fiscal year 1999, recommended to the Commission (and received approval for) additional research studies on LPSD operations. As a result, this program was initiated in early 1999.

1.2 Objective

The objective of this program is to provide (or develop, as necessary) an understanding of the risk associated with accidents during LPSD operations sufficient to support risk-informed regulatory activities. These activities include inspection and enforcement, events assessment, maintenance rule, Regulatory Guide 1.174, and risk-informing part 50.

The objective of this report is to provide recommendations on research needs to accomplish the program's objective. In support of this objective, perspectives on LPSD risk were developed and documented. Perspectives are provided in the following areas:

- **An understanding of the significance of LPSD risk**
  - risk importance of LPSD in terms of core damage frequency (CDF) and public health risk
  - types of initiating events that can challenge the plant during LPSD conditions
  - major contributors to LPSD CDF and public health risk (e.g., dominant initiating event frequencies and dominant failures)
  - plant operating states contributing to LPSD CDF and public health risk (e.g., hot shutdown)

- **Understanding of current domestic LPSD risk methods and tools**
  - S principal use for which the methods and tools were developed and associated metrics
  - S underlying technical approaches used (e.g., small event/large fault tree, definition of plant operational state, use of existing full-power models, data, human reliability analysis (HRA))
  - S scope of the events (e.g. internal, external) modeled and types of outages modeled
  - S level of detail modeled (e.g., components, failure modes, dependencies)

- **Ability of current methods and tools to support risk-informed regulatory activities**
  - types of LPSD risk assessments needed to support risk-informed activities
    - qualitative, quantitative, non-PRA assessments
    - plant-specific PRA assessments
  - strengths of methods and tools
  - weaknesses of methods and tools

- **Recommendations with proposed schedule and resources**
  - guidance development
  - method and tool development
  - support for the development of a consensus standard

1.3 Approach

In developing the above perspectives, the following tasks were performed:

(1) Collect information from available resources. This task involved:
  - search of literature and databases
  - issuing a questionnaire to support the information-gathering process
  - holding a public workshop to solicit information from the industry and other stakeholders
  - meeting with licensees and consulting engineering firms to develop a better understanding of methods and tools currently available for managing LPSD risk.

(2) Analyze information. This task involved the evaluation of information gathered with respect to:

- strengths and limitations of existing information, processes for assessing LPSD risk, and applicability to the majority of the operating plants
- identification of limitations that would not permit extrapolation of available data to assess the risk of LPSD across plants
- strengths and weaknesses of existing methods and tools to support risk-informed regulatory activities

(3) Develop Recommendations. This task involved the identification of:

- approaches that could be used to incorporate risk into the regulatory activities
- methods and tools needed in these approaches
- areas where existing methods and tools are insufficient or incomplete
- type of work needed to improve the methods and tools (guidance, method, and tool development
- prioritization of "research" issues
- resources and schedule

1.4 Scope and Limitations

The objective of this effort was to develop an understanding of LPSD risk *sufficient* to support risk-informed regulatory activities. Therefore, it focused on gathering information adequate to develop this understanding (which includes the significance of LPSD risk and methods and tools available to assess it.) The staff did not perform an exhaustive search and evaluation of LPSD risk studies, methods, and tools. Furthermore, the information was evaluated as reported. That is, the staff did not examine whether existing methods and tools do indeed have the capabilities presented or how accurately these methods or tools are applied.

1.5 Report Organization

Chapter 2 presents the perspectives on the significance of LPSD risk; Chapter 3 provides perspectives of currently-available LPSD methods and tools; Chapter 4 discusses the strengths and weaknesses of LPSD methods and tools for supporting risk-informed regulatory activities; and Chapter 5 provides recommendations on future work and a multiyear plan with individual tasks and milestones.

REFERENCES

1.1 D. W. Whitehead et al., “Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1: Summary of Results,” NUREG/CR-6143, SAND93-2440, Vol. 1, Sandia National Laboratories, Albuquerque, NM, July 1995.

1.2 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, Vols. 1-6, Brookhaven National Laboratory, 1994.

1.3 U.S. Nuclear Regulatory Commission, “Loss of Residual Heat Removal System, Diablo Canyon, Unit 2,” April 10, 1987

1.4 U.S. Nuclear Regulatory Commission, “Loss of vital AC power and the Residual Heat Removal System During Mid-Loop Operations at Vogtle Unit 1 on March 20, 1990,” May 1990.

1.5 U.S. Nuclear Regulatory Commission, “Issuance For Public Comment Of Proposed Rulemaking Package For Shutdown and Fuel Storage Pool Operation,” SECY-97-168.

1.6 U.S. Nuclear Regulatory Commission, “Staff Requirements - SECY-99-063-The use by Industry of Voluntary Initiatives in the Regulatory process,” May 27, 1999.

1.7 Nuclear Management and Resources Council, Inc., “Guidelines for industry Actions to Assess Shutdown Management,” NUMARC 91-06, 1991.

1.8 USNRC, “Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement,” *Federal Register,* Vol. 60, p. 42622, August 16, 1995.

1.9 Letter from R.L. Seale, Chairman, Advisory Committee on Reactor Safeguards, to Chairman Shirley Ann Jackson, USNRC, “ Establishing a Benchmark on Risk During Low-Power And Shutdown Operations” April 18, 1997.

1.10 U.S. Nuclear Regulatory Commission, “An Approach for Using PRA Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” Regulatory Guide 1.174, July 1998.

2. THE SIGNIFICANCE OF LPSD RISK

This section provides perspectives on the significance of low power and shutdown (LPSD) risk obtained from a review of LPSD operational events and LPSD risk and related studies performed by either the Nuclear Regulatory Commission (NRC) or industry, both domestic and international.

Perspectives regarding the significance of LPSD risk are summarized below in Table 2.1.

Table 2.1 Summary of perspectives on LPSD risk significance.

- Potentially significant operational events occur.
- Risk from LPSD conditions can be comparable to full power.
- LPSD risk at boiling water and pressurized water reactors appears to be dominated by three classes of initiating events (loss of shutdown cooling, loss of coolant, and loss of offsite power).
- Dominant failures associated with LPSD events appear to be human-related.
- The most risk dominant plant operational states are characterized by high decay heat and reduced inventory.
- Risk contributors appear to be very plant-specific.
- Initiating events that have been analyzed for full power conditions must be reexamined to ensure that all LPSD effects are considered.
- Outages other than for refueling may be important contributors to risk.

These perspectives are discussed in further detail below.

2.1 Perspectives from Operational Events

Numerous events that are potentially risk-significant have occurred at U.S. plants during LPSD conditions. These events have required mitigation with plant safety systems to prevent core damage. These events combined with the plant response provide relatively high estimated conditional core damage probabilities (1E-4 to 1E-3) and therefore, from a risk perspective, warrant consideration. In other words, initiating events unique to LPSD suggest the contribution to risk during LPSD from the design and operation of the plant is significant. Table 2.2 summarizes perspectives obtained from reviewing events that have occurred since 1987.

Table 2.2 Summary of perspectives on LPSD events.

- Similar events are occurring across the industry.
- The events have generally involved:
  - loss of shutdown cooling,
  - loss of coolant,
  - loss of offsite power, and
  - loss of power supplies other than those initiated by loss of offsite power.
- The specific causes of the events tend to be plant-specific.
- The majority of the events include human factors involving:
  - personnel errors, and
  - deficient procedures.
- Plant configuration and/or incomplete operator knowledge may contribute to an event and may limit the capability to mitigate an event.

Five LPSD events that illustrate many of the above perspectives are briefly discussed below.

Vogtle Loss of Vital AC Power Event–3/20/90

A loss of offsite power occurred when a truck driver backed into a support pole for the C phase of the 230-kV feeder line supplying offsite power–a human error. Prior to the event, the plant was in the 24th day of a scheduled 44-day refueling outage with the water level at mid-loop, decay heat was being removed by residual heat removal (RHR) train A, and diesel generator (DG) B was out for maintenance. Upon loss of offsite power, DG A started to supply emergency loads (e.g, RHR train A), but tripped and locked out, as it was designed to do, after approximately 80 seconds. The trip and lockout were unexpected by the operators, and 18 minutes were spent responding to the event. The A diesel generator was restarted, but tripped again after 70 seconds. Another 15 minutes were spent investigating the cause of the trip; however, the operators were again unsuccessful in determining the cause of the trip. At this time (36 minutes into the accident), the operators restarted the A diesel generator using the manual emergency start, and the diesel generator continued to run until removed from service by the operators after offsite power had been restored (approximately 3 hours after the start of the event). During the time DG A was not operating, decay heat removal was unavailable, resulting in 46°F rise (90 to 136) in temperature.

Wolf Creek Drain Down Event–9/17/94

A loss of reactor coolant was caused by an inadvertent blowdown to the refueling water storage tank (RWST) through the RHR system. Operators had failed to identify this flow path, and consequently, during the cooldown phase to begin a refueling outage, the operators opened RHR valves that inadvertently permitted this blowdown to occur. If this loss of reactor coolant had not been mitigated, the hot leg would have uncovered, introducing steam into the RWST header line (the water supply line for the emergency core cooling system (ECCS) pumps) and resulting in the subsequent common-mode failure of the ECCS pumps, if operated. Failure of the ECCS pumps would have resulted in core uncovery in about 30 minutes. However, operators terminated the blowdown in about one minute (a relief crew supervising operator identified the flow path and informed an operator that a valve should be closed).

Cooper Human Action Renders RHR Loop A Inoperable Event–12/2/98

A problem occurred during maintenance activities that rendered Loop A of the RHR system inoperable. Operators failed to realize that concurrent activities, maintenance on the loop A room cooler and coverage of 75% of a loop A natural circulation opening, rendered loop A pumps inoperable. If an initiating event that resulted in the loss of the other train of RHR had occurred, the plant would have been forced to respond to the event in a degraded state.

Clinton Loss of Shutdown Cooling Event–2/13/98

An inadvertent isolation of shutdown cooling occurred when a common line suction valve for the RHR system closed, resulting in the loss of all shutdown cooling. The valve closed when a 12 vdc power supply that was a load to the Division II Nuclear Systems Protection System (NSPS) bus failed. The NSPS inverter, sensing the failure of the power supply, reverse-transferred to the bypass transformer (an alternate supply); however, since the bypass transformer was out of service for maintenance, the bus lost power and subsequently caused the RHR suction valve to shut, resulting in the loss of shutdown cooling. Operators were able to reopen the valve when the bypass transformer was returned from maintenance, thus preventing the need for using alternate decay heat-removal mechanisms to prevent core damage. The root cause of the event was the lack of a contingency plan when placing the bypass transformer out of service for maintenance.

Washington Nuclear Plant - Unit 2 Flooding of ECCS Event–6/17/98

During cold shutdown, a water hammer event occurred in the plant fire protection system piping that resulted in the flooding of RHR pump room C (water flooded a stairwell to a level sufficient to cause deformation and failure of the fire door leading to an adjacent vestibule from which flood water entered the RHR C room through the water-tight door, which had not been properly dogged closed) and the subsequent flooding of the low pressure core spray (LPCS) pump room when an RHR pump C room floor drain isolation valve failed to automatically close, providing a flow path from the RHR C room sump to the floor drains in the LPCS room. Since both RHR trains A and B remained available during this event, the event might not be considered important, except that a subsequent review of the plant's flooding analysis revealed that flooding of this magnitude is outside the plant's design basis. This, coupled with the human-related failure to maintain the integrity of water-tight doors, raises the potential importance of events like this during shutdown conditions.

The list of events in Table 2.3 indicate that potentially important events do occur.

Table 2.3 Shutdown events occurring during 1998 and the early portion of 1999.

Initiating Event Class	Plant/ Date	Event Description/Consequences
Loss of Shutdown Cooling	Limerick 1 2/6/98	Loss of shutdown cooling and mode change. Fuse blew while installing a jumper, causing RHR to isolate. Primary coolant system temperature increased from 191^{o}F to 200^{o}F, changing modes from cold shutdown to hot shutdown.
	Clinton 2/13/98	Loss of shutdown cooling due to loss of nuclear safety Div II. An alert was declared in order to activate the Technical Support Center and to provide for more manpower.
Loss of Coolant	ANO 2 2/2/99	Inadvertent entry into reduced inventory operations. Reactor vessel level dropped 56 inches within approximately 1.5 minutes.
	Quad Cities 2 2/24/99	A draindown event occurred as a result of switching from train B of RHR shutdown cooling to train A when operators failed to perform tasks in the correct order. Water level was reduced from 80 inches indicated to about 45 inches indicated (a loss of approximately 6000 to 7000 gallons).
	FitzPatrick 12/2/99	An operator-induced 100-inch (approximately 14,000 gallons) draindown event occurred when operators attempted to maintain indicated water level at 357 inches above the top of the active fuel using a level instrument with a temporary addition to its reference leg. This temporary addition was in the process of being replaced with the original reference leg components. This replacement activity increased the indicated level, and the operators compensated for this apparent increase in level by increasing the discharge rate.
Loss of Offsite Power	Ft. Calhoun 5/20/98	Transformer explosion results in Loss-of-offsite power (LOOP). Emergency diesel generators (EDGs) start and load. SD cooling interrupted for several seconds. No heat up (time to boiling–2 hours).
	McGuire 1 6/3/98	Explosion of switchyard breaker and LOOP. (1E power was supplied through U2.)
	Clinton 1/6/99	LOOP; EDGs started and loaded. Shutdown cooling via RHR lost. Fourth of four events involving loss of shutdown cooling. B-RHR tripped and shutdown cooling was supplied via RWCU.
Loss of Power	Clinton 6/29/98	Loss of 3 of 4 offsite power sources due to storm damage. Shutdown cooling B-pump tripped; restarted. Spent fuel pool cooling lost. Spent fuel cooling and one shutdown cooling bus lost. Shutdown cooling was restated without reactor coolant system (RCS) heatup. Spent fuel cooling restored.
	D.C. Cook 1&2 8/31/98	Train A reserve power supply lost due to loss of station service transformer. EDGs for train A, both units, auto-started. Operating RHR pump, each unit, briefly lost with no heatup of RCS.

Table 2.3 Shutdown events occurring during 1998 and the early portion of 1999.

Initiating Event Class	Plant/ Date	Event Description/Consequences
	Catawba 2 9/6/98	Loss of 4160 V bus, auto start of one auxiliary feedwater (AFW) pump, and lifting of one power-operated relief valve (PORV). The plant was preparing to go water solid; therefore, little space was available in the pressurizer to accommodate the increase in RCS volume. When the charging pump discharge valve went full open, the increase in flow caused the PORV to lift about 12 to 14 times. One 1E bus lost power and was not loaded by its EDG since the EDG was down for maintenance. The fuel was not in the core.
	San Onofre 2 2/1/99	Loss of shutdown cooling due to breaker malfunction. Inadequate pre-job briefing, inadequate work plan, and inadequate controls of work in progress lead to three-phase fault with normal clearing while working on breaker and 2 °F RCS temperature rise.
Fire	Fermi 2 10/8/98	Fire in EDG panel. Damage was limited to the panel. Cause not stated.
	Fermi 2 10/10/98	Fire in a motor control center in Rad Waste. Second electrical fire in two days. This was caused by personnel error and resulted in personnel injury.
Flood	WNP 2 6/17/98	Fire header line break with subsequent flooding of ECCS pump rooms. ECCS pumps rendered inoperable by flooding.
Other	WNP 2 5/30/98	Full scram and injection of LPCS, low-pressure coolant injection (LPCI) A start, start of Div I and III EDGs (accident signal response). 2600 gallons of water were injected, increasing RCS pressure and decreasing temperature. Pressure increased from 107 psig to 425 psig. Temperature decreased from 222 °F to 219 °F.
	WNP 2 5/31/98	Scram while shut down. Reactor pressure increased from 1034 psig to 1064 psig. Recurring problem. Possible cause is scram discharge volume level high.
	Salem 1 2/21/98	Operator inattention resulted in start of AFW to feed steam generator (SG). AFW ran with discharge valves closed for less than one minute. AFW was not required to be operational in the current mode, did not feed the steam generators because the feed valves were closed. Level in SGs was supposed to be maintained between 18% and 28%, but got to 9% of narrow range.
	Limerick 2 6/3/98	Standby liquid control injected into the vessel. Between 300 and 350 gallons of water bearing B4C injected. Unnecessary injection of B4C necessitated cleanup of RCS. B4C could damage carbon steel components in RCS.
	Clinton 6/10/98	Service water pump flow indications at RHR heat exchanger (HX) off-scale high. HX bypass line inadequately sized so that high flow would occur in the line should the HX be bypassed and inadequate cooling to other safety-related components could occur.

Based on the operational events that have occurred since the early 1980s, initiating events during LPSD conditions are occurring that could be risk significant. Therefore, it is important to determine the following:

- Are there other potential initiating events?
- What is the risk significance of the events (e.g., core damage frequency (CDF))?
- What are the contributors, or what are the most likely scenarios that could escalate to core damage, if the initiating event has occurred?
- What are the most likely conditions under which the initiating events will occur (e.g., operating modes)?

Perspectives regarding the questions are provided based on current LPSD risk assessments and selected studies.

2.2 NRC LPSD Risk Studies

LPSD risk and related studies have been performed by the NRC (References 2.1–2.7). Results from these studies are summarized in the following sections. Table 2.4 provides a summary of the perspectives from the NRC studies. A discussion of perspectives from each study follows.

Table 2.4 Summary of perspectives from the NRC LPSD risk and related studies.

- Important initiating events include
  - loss of shutdown cooling,
  - loss of coolant,
  - loss of offsite power, and
  - internal fires
- Core damage frequency and risk estimates can be comparable to full power values.
- Human actions and the uncertainty associated with them are major contributors to LPSD risk.
- Dominant accident sequences usually involve plant conditions where:
  - decay heat is still high,
  - water level is reduced, and/or
  - equipment is being maintained.
- The more important plant operational states (POSs) have the same characteristics as the dominant sequences.
- Conditional LPSD risk (per hour) is comparable (or higher) than conditional full power risk.
- Conditional (per hour) risk cannot be directly scaled to risk per year (risk based on being in a plant operational state (POS) for a full year).
- Physical separation of equipment is an important factor in determining whether fire or flood will be important to risk.
- Equipment design and plant location are important factors in determining the significance of seismic events.
- Transition risk (i.e., risk associated with shutting down a plant to accomplish some activity) associated with repair of failed equipment can exceed the risk associated with continuing to operate while repairing the equipment.

2.2.1 Grand Gulf LPSD Risk Assessment

An assessment of the risk of the Grand Gulf plant (a boiling water reactor (BWR) 6 reactor, Mark III containment) during low power and shutdown conditions was performed (Ref. 2.1). This analysis considered the identification and consequence of the potential initiating events that could occur during different low power and shutdown operating states. The following perspectives were identified from an examination of the results.

Plant operational states with high decay heat, equipment out of service, and low water inventory are more risk-significant. POS 5 (cold shutdown) and POS 6 (refueling where the water level has been raised to the steam lines) are the most risk-significant (when looking at their core damage frequencies), respectively. The contribution to CDF from the other POSs is negligible–a 2.7% contribution. During these states (i.e., POSs 5 and 6), the decay heat is still relatively high, equipment is being maintained, and vessel inventory (i.e., water) has not been connected to the upper pool; therefore, accident sequences initiated during these states tend to be more important than those initiated during other POSs.

Fire, flood, and seismic events are not important at Grand Gulf because of physical separation (fire and flood) and plant design and location (seismic). These events are much less important than internal events (the mean CDFs from fire, flood, and seismic range from a factor of 30 to more than a factor of 100 less than the CDF from the remaining internal events). Fire and flood are not important because of the good physical separation between trains of equipment at Grand Gulf. Seismic is unimportant because Grand Gulf's seismic capacity is well above its design basis and the Grand Gulf site is located in one of the least seismically-active locations in the United States.

Dominant contributors to core damage frequency involve loss of coolant and loss of offsite power events with failures (human and/or hardware) that cut across multiple system boundaries. Within the internal events analysis where fire and flood were excluded, two groups of initiating events were important: 1) loss-of-coolant/diversion of inventory events and 2) loss of offsite power (LOSP)/blackout events. For the loss-of-coolant/diversion events, operator failure to control reinjection of water into the vessel results in the loss of all means of injection, thus leading to core damage. For the loss of offsite power events, operators failing to recover offsite power or the non-maintained diesel generator failing to run results in multiple systems/trains being unavailable, thus leading to core damage.

The average risk at Grand Gulf as it operates in POS 5 during a refueling outage is comparable with the risk associated from full power operation. [3] On a per calendar year basis, the average risks (core damage frequency, early fatality risk, and total latent cancer fatality risk) are comparable for POS 5 as for full power internal events (fire and flood excluded):

	POS 5	Full power[4]
CDF	2E-6	4E-6
Early fatality (total) risk	1E-8	8E-9
Total latent cancer risk	4E-3	1E-3

The most likely accidents in POS 5 have the following characteristics:

- an open containment,
- the suppression pool is bypassed,
- the containment sprays are not available, and
- the vessel fails, releasing the core debris into the containment.

The low values for risk given the high conditional releases are, in part, due to the extremely low core damage frequency and the sparse population around the plant.

[3] In estimating early fatality (total) risk and total latent cancer risk, no LPSD-specific modifications were made to the source term except to account for decay based on the time from reactor shutdown.

[4] Estimates on a per calendar year basis take into account the fraction of time on average the plant spends in each state (e.g., POS 5 and full power) during any one year. For the Grand Gulf POS 5 analysis, the fraction of time the plant is in POS 5 is 0.031. The full power CDF value uses 1.0 as the fraction because the analysis calculated CDF on a per-reactor-year basis. In reality, the comparison should made with the fraction of time associated with full-power operation (something close to 0.8) included in the CDF value. However, this small difference is not expected to significantly affect any comparisons made and is therefore ignored.

The conditional POS 5 risk at Grand Gulf is more significant than conditional full power risk because of the increased complexity of operator actions. On a per hour basis, the conditional risks for POS 5 are higher than the conditional risks for full power operation:

	POS 5	Full power
CDF	7E-9	5E-10
Early fatality (total) risk	5E-11	9E-13
Total latent cancer risk	1E-5	1E-7

POS 5 has a higher risk contribution because, although there is lower decay heat that provides the operators with more time to deal with events (given an initiating event), many of these operator actions are more involved and complicated than at full power. In POS 5, a reduced set of equipment is available to the operators in responding to the event because of the required test and maintenance activities.

To avoid overestimating the risk from being in POS 5 for one year, per hour results from the POS 5 analysis should not be directly scaled. In other words, one *cannot simply multiply* the per hour results by the number of hours in a year and have the correct estimation of either CDF or risk for a POS 5 year. Such a process would overestimate the CDF and risk for POS 5 for the following three reasons:

1. The decay heat load would continue to decrease during the year, resulting in additional time for the operators to respond to any undesired event.

2. The unavailability associated with the systems would change as the year progressed, generally getting smaller, and thus reducing the likelihood of an accident progressing to core damage as a result of equipment unavailability.

3. Decay would reduce the radiological inventory that is available to cause health effects.

2.2.2 Surry LPSD Risk Assessment

An assessment of the risk of the Surry plant (a Westinghouse 3-loop reactor, large dry subatmospheric containment) during low power and shutdown conditions was performed (Ref. 2.2). This analysis considered the identification and consequence of the potential initiating events that could occur during the different low power and shutdown operating states. The following perspectives were identified from an examination of the results.

Plant operational states with reduced water inventory are more risk-significant. POS 6 (mid-loop before refueling and for drained maintenance) and POS 10 (mid-loop after refueling) are the most risk-significant (when looking at the combination of core damage frequency and major release factors). During these states, vessel inventory (i.e., water) has been reduced to approximately the mid-point of the reactor coolant system injection nozzle; therefore, accidents initiated during these states tend to be more important than those initiated during other POSs.

Internal fire events are the most important events at Surry because of physical separation issues. Fire is important because a single fire at a few critical locations could damage almost all the equipment needed to mitigate an accident.

Seismic events are the least important events at Surry because of design and location. Seismic is the least important because Surry's seismic capacity is well above its design basis and the Surry site is located in one of the least seismically-active locations in the United States.

Dominant contributors to core damage frequency involve initiating events that cut across multiple system boundaries and human errors (i.e., failure of the operators to mitigate the accident). The dominant contributor to core damage is operator failure to mitigate accidents. In addition, as stated above, a single fire at critical locations can damage almost all the equipment needed to mitigate an accident. Furthermore, certain flood initiators can result in multiple equipment failures. For internal events (excluding fire and flood), two classes of initiators are the most important: 1) loss of RHR events, and 2) LOSP/blackout events.

The average total latent cancer risk at Surry as it operates in mid-loop conditions is comparable with the risk from full power operation.[5] On a per-calendar-year basis, average total latent cancer fatality risk for internal events (excluding fire and flood) for mid-loop is comparable with full power:

	Mid-loop	Full power[6]
CDF	5E-6	4E-5
Early fatality (total) risk	5E-8	2E-6
Total latent cancer risk	2E-2	5E-3

Mid-loop risk is comparable to full power risk because the containment is most likely to be unisolated for a significant fraction of the accidents initiated during mid-loop operation. This results in releases to the environment that are potentially large and comprised of radionuclide species that contribute to long-term health effects (such as cesium) because they have long half-lives, and thus experience no appreciable decay since the reactor was shutdown.

The conditional mid-loop risk at Surry is at least comparable to the conditional full power risk. On a per hour basis, the conditional mid-loop risks are at least comparable to the conditional full power risks:

	Mid-loop	Full power
CDF	9E-9	5E-9
Early fatality (total) risk	8E-11	2E-10
Total latent cancer risk	3E-5	6E-7

Mid-loop is at least comparable because, although there is lower decay heat that gives the operators more time to respond to events (given an initiating event), many of these operator actions are more involved and complicated than those at full power. In mid-loop, a reduced set of equipment is available to the operators in responding to the event because of the required test and maintenance activities, and the containment is usually open.

[5] In estimating early fatality (total) risk and total latent cancer risk, no LPSD-specific modifications were made to the source term except to account for decay based on the time from reactor shutdown.

[6] Estimates on a per-calendar-year basis take into account the fraction of time on average the plant spends in each state (e.g., POSs 6 and 10 and full power) during any one year. For the Surry analysis, the following fractions were used:

R6 (POS 6 for a refueling outage)	= 0.0163,
D6 (POS 6 for a drained maintenance outage)	= 0.0349,
R10 (POS10 for a refueling outage)	= 0.152, and

The full power CDF value uses 1.0 as the fraction because the analysis calculated CDF on a per-reactor-year basis. In reality, the comparison should made with the fraction of time associated with full-power operation (something close to 0.8) included in the CDF value. However, this small difference is not expected to significantly affect any comparisons made and is therefore ignored.

2.2.3 Other NRC Risk-Related Studies

<u>Loss of RHR in PWRs (NUREG/CR-5015)</u>

A generic PWR shutdown risk study was performed (Ref. 2.3). This analysis examined the consequences from three classes of initiating events:

- loss of shutdown cooling,
- loss of coolant, and
- loss of offsite power.

From this analysis, the following perspectives were identified.

Risk during shutdown is comparable with the risk associated from full power operations. The estimated CDF at shutdown, 5E-5 per reactor year, from the generic PWR shutdown study is comparable with the individual plant examination (IPE) estimates of CDF during full power conditions for PWRs (approximately 5E-4 to 4E-6 per reactor-year) (Ref. 2.4).

Within the three classes of initiating events examined, one class of initiating events (i.e., loss of shutdown cooling) and one plant condition (i.e., reduced water inventory) dominate the CDF results. The loss of shutdown cooling initiating events contributes more than 80% of the total CDF. The reduced water inventory condition accounts for about 65% of the total CDF.

Human error during reduced water inventory conditions is the dominant failure contributor to CDF. Operator failure to diagnose that a loss of cooling has occurred and to successfully restore it while at reduced inventory in the reactor coolant system accounts for about 65% of the total CDF. The major reason for the significance of human actions is that the reduced inventory condition minimizes the amount of time the operators have to diagnose and correct any failures.

<u>Core Melt Probability from Postulated Loss-of-Coolant (LOCA) During Cold Shutdown (SAI0182-147LJ, Rev.1)</u>

An analysis of postulated loss-of-coolant accidents (LOCAs) initiated by a safe-shutdown seismic event or an operator error was performed for the Sequoyah plant (Ref. 2.5). The analysis examined 20 cases with varying assumptions regarding the cause (i.e., seismically- or human-induced), timing (i.e., time after shutdown), size (i.e., break size) of the initiating event, maintenance status (i.e, whether significant maintenance is occurring), and availability of offsite power (during 100-hour period following the initiating event). From this analysis, the following perspectives were identified.

Risk of a LOCA during shutdown (either operator- or seismically-induced) can be comparable with the risk associated from internal full power LOCAs. The range of the estimated CDF (core melt frequency in the report) for LOCAs at shutdown resulting from an operator error is 1E-7 to 8E-5 per reactor-year. Comparing these results with the IPE LOCA results from full power (2E-5 per reactor year), it appears that risk during shutdown can be comparable to risk during full power operation. For seismically-induced LOCAs, the range of estimated CDF is 7E-7 to 6E-5 per reactor year. Thus, seismically-induced LOCA risk can also be comparable to internal full power LOCA risk.

The dominant contributors to CDF (human error and equipment/support failure) involve significant uncertainty. For human errors (either operator-induced LOCAs or response errors), the uncertainty is such that it is unclear how the results would be affected (i.e., increase or decrease the CDF). For equipment/support failures (e.g., failure of an airbound RHR pump), the most likely result of a decrease in uncertainty would be a reduction in the estimated risk.

Technical Specification Action Statements Requiring Shutdown (NUREG/CR-5995)

An approach for assessing the risk contribution from shutting down a plant to repair inoperable equipment (transition risk) to that of repairing the inoperable equipment while the plant continues operating at power (continued operation risk) was developed and applied to the RHR and standby service water (SSW) systems of a BWR/6 plant (Ref. 2.6). The following perspectives were identified from an examination of the results.

The risk associated with shutting down the plant for an RHR or SSW failure can exceed the risk from continued operation. For single and double RHR failures, shutdown risk exceeds continued operation risk for approximately two and six days, respectively. For SSW failures, shutdown risk exceeds continued operation risk for a minimum of three days.

SSW transition risk and continued operation risk are higher than the same risks for a front-line system because of the dependencies associated with the support system. Cumulative risk, for any specified amount of time, associated with SSW system failures is greater than the same risk for RHR system failures. This is because, generally, support system failures result in failure of more than one system while failure of a front-line system is self-contained.

Action Requirements for AFW System Failures (NUREG/CR-6502)

Using an approach similar to Reference 2.6, NUREG/CR-6502 (Ref. 2.7) assessed the transition risks associated with the auxiliary feedwater (AFW) system at four PWRs. The following perspective was identified from an examination of the results.

For a repair time of 24 hours, the risk associated with shutting down the plant for AFW failures exceeds the risk from continued full-power operation. For continued operation, the CDF increases in value due to the loss of function of the failed equipment and remains at this value until the equipment is repaired. For the shutdown option, two peaks occur with an overall decreasing trend as time elapses from shutdown. The first peak occurs immediately following shutdown when the plant is vulnerable to transients primarily involving loss of feedwater and loss of offsite power and when the time to steam generator dryout is short. From this point, CDF decreases because of the decreasing decay heat load and the subsequent increase in operator response time until the changeover from hot standby to hot shutdown. At this point, another peak occurs because of the possibility of an interfacing system LOCA and the possible failures to start the RHR system to remove decay heat in case of multiple failures in the AFW system. Using a repair time of 24 hours, estimates of shutdown risk versus continued operation risk (a ratio) ranges from about 4 to 300, depending on the number of initial AFW failures.

2.3 Domestic LPSD Industry Studies

This section discusses perspectives obtained from a review of industry-initiated risk studies of LPSD conditions for domestic nuclear power plants (References 2.8–2.16). Table 2.5 provides a summary of the perspectives from this review. A discussion of perspectives from each study follows.

Table 2.5 Summary of perspectives from the industry-initiated LPSD risk and related studies.

- Core damage frequency estimates can be comparable to full power values.
- Risk estimates (large early release frequency (LERF) and early fatalities) show no clear pattern; however, status of the equipment hatch is an important risk factor.
- Important initiating events include:
  - — loss of shutdown cooling,
  - — loss of coolant, and
  - — loss of offsite power.
- Human actions and the associated uncertainty are major contributors to LPSD risk.
- Dominant accidents sequences usually involve plant conditions where:
  - — decay heat is still high,
  - — water level is reduced, and/or
  - — equipment is being maintained.
- Transition risk (i.e., risk associated with shutting down a plant to accomplish some activity) associated with repair of failed equipment is comparable to the risk associated with continuing to operate while repairing the equipment.

Low Power and Shutdown Workshop

On April 27, 1999 the NRC sponsored a LPSD Workshop to solicit information related to the risk associated with low power and shutdown conditions (Ref. 2.8). During the workshop, industry personnel made several presentations that contained results from analyses of low power and shutdown conditions. Major perspectives from the Workshop are discussed below.

CDF risk estimates indicate that shutdown risk can be comparable to that from full power. Results from the use of shutdown Safety Monitor™ models for a refueling outage for one of the member of the Safety Monitor™ Users Group indicated that outage risk is on the order of Level 1 risk, 1E-5 per year contribution to cumulative risk. At River Bend, equipment out-of-service (EOOS) shutdown PRA analyses indicated that shutdown risk is comparable to at-power risk (e.g., cumulative risk for a 21-day outage could be as high as the yearly at-power risk). At South Texas, outage risk assessment and management (ORAM) shutdown PRA analyses indicated that risk during refueling (approximately 4E-5) is comparable to at-power risk (i.e., same order of magnitude). The Seabrook Shutdown PRA indicated that the mean CDF is in the same range as the at-power CDF. According to the Electric Power Research Institute (EPRI), results from the analysis of a typical BWR outage indicated that risk is approximately 6E-7 per year while the analysis of a typical PWR outage indicated that risk is approximately 2E-5 per year.

For Level 2 and 3 risk measures (LERF and early fatalities), no clear patter emerges. The Seabrook Shutdown PRA indicated that no early fatalities occur assuming a realistic source term and at least a two-mile evacuation zone. However, an analysis of the AP600 reactor design indicated that the shutdown LERF was approximately 25% of the at-power value.

Four factors (i.e., low water level, time since shutdown, human error, and maintenance of support systems) are important to shutdown CDF risk. An analysis of the AP600 reactor design indicated that 85% of the shutdown CDF comes from events during drained (i.e., low water level) conditions in the reactor coolant system. Results from a Safety Monitor analysis indicated that most of the cumulative risk of shutdown comes from low inventory configurations, configurations early in the outage, and plant operational states of long duration, i.e., more than a few hours. Results from an EOOS shutdown analysis at River Bend indicated that core damage frequency is driven by maintenance of support systems. The Seabrook Shutdown analysis identified two times of greatest concern with the water level; level at the flange and level at mid-loop. Both result in a low thermal margin, while mid-loop also results in a low margin-to-RHR pump cavitation. The Seabrook analysis also indicated that shutdown risk is difficult to quantify because of the importance of human actions and the difficulty in correlating response time versus human reliability. From EPRI analyses, more than 50% of the average shutdown CDF is due to human errors that occur during peak periods of conditional risk.

Most CDF risk occurs during peaks–times of high conditional CDF that are usually short in duration. According to EPRI, approximately 85% of the average shutdown CDF risk for a typical BWR or PWR outage comes from the risk peaks that occur during an outage.

Accidents that are important to release (and ultimately to public risk) are those where the equipment hatch is off (or open). The Seabrook analysis found that accidents where the equipment hatch is off are most important to release.

Using currently available methods and tools, plants have found risk-significant operational states. In their efforts to track and manage shutdown risk (mainly from refueling outages), plants are using currently-available methods and tools. Use of these methods and tools has shown that plants go through risk significant configurations or operational states during refueling outages (e.g., Figure 2.1 indicates that states with reduced water inventory can be risk-significant). Identification of these risk-significant states allows the plants to control and minimize the risks from these states.

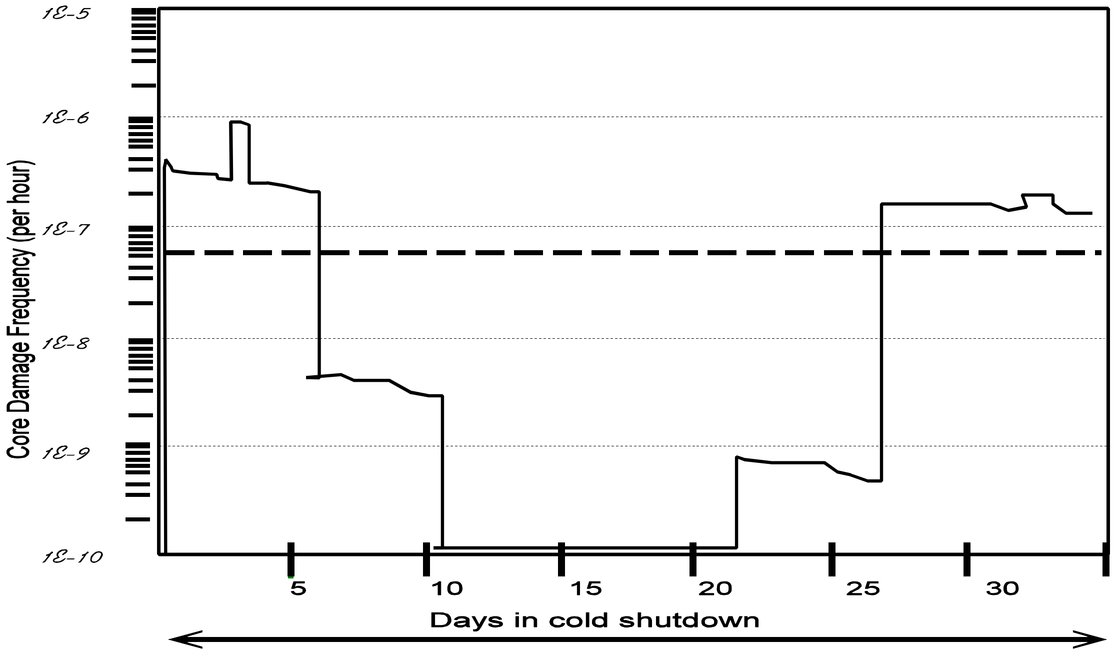

Figure 2.1 Example of CDF profile of plant during cold shutdown.

Zion Residual Heat Removal PRA (NSAC-84)

The NSAC-84 study (Ref. 2.9) extended the Zion Probabilistic Safety Study (Ref. 2.10) to address the risk at Zion during the entire time the plant is in cold shutdown conditions by quantifying core damage frequency (and other safety concerns) for initiating events identified in a generic PWR decay heat removal review (i.e., NSAC-52) and to look for other contributors to shutdown risk. From this analysis, the following perspectives were identified.

Risk during shutdown is comparable with the risk associated from full power operations. The mean shutdown CDF of 1.8E-5 per year is more than 25% (27%) of the power operations CDF of 6.7E-5 per year. The uncertainty in the core damage frequency for shutdown is greater than the uncertainty for power operations. Given the uncertainties involved for shutdown, the risk of fuel damage during some periods of a shutdown may be as great as the at power risk.

The dominant contributor to core damage frequency and its uncertainty is human error. Human errors contribute to all core damage scenarios. Failure of the operator to respond during reduced-inventory operation accounts for almost 45% (44%) of the total CDF. The operator's failure to determine the proper actions to restore shutdown cooling accounts for slightly more than 55% (56%) of the total CDF. The uncertainty associated with producing human error estimates for shutdown conditions contributes significantly to the uncertainty in core damage frequency. The uncertainty associated with human error estimates is greater than the uncertainty associated with hardware failures.

Brunswick Decay Heat Removal PRA (NSAC-83)

The NSAC-83 study (Ref. 2.11) performed a probabilistic evaluation of the reliability of the decay heat removal system for scenarios where the temperature of the suppression pool reached 200°F–the endstate of interest–resulting from events initiated from full power operation and from events occurring during cold shutdown. Results from this endstate analysis were then extrapolated to produce estimates of core damage frequency for each initiating event. From this analysis, the following perspective was identified.

Risk from events initiated from power that ultimately involve loss of decay heat removal are more important that the risk from events initiated during cold shutdown. The frequency of reaching the 200°F-endstate for events initiated during power operation (approximately 4E-5 per year) is greater than the risk from events initiated during cold shutdown (approximately 7E-6). Extrapolating these results to core damage risk, events during power operation (approximately 4E-6) are still more important than events during cold shutdown (approximately 5E-7).

Seabrook Station Probabilistic Safety Study, Shutdown (modes 4, 5, and 6)

The Seabrook shutdown analysis (Ref. 2.12) estimated the core damage frequency and public risk of accidents that could occur while the plant is operated in modes 4 through 6 (i.e., hot shutdown, cold shutdown, and refueling). From this analysis, the following perspectives were identified.

Risk (i.e., CDF) from shutdown operations is comparable to full power risk. The total shutdown CDF was estimated to be 4.5E-5 per reactor year. This is approximately 40% of the total full-power CDF from Seabrook's IPE (1.1E-4 per reactor year).

The contribution to risk (i.e., CDF) from initiating events is dominated by loss of RHR, and loss of RHR is dominated by internal events that exclude fire and flood. Loss of RHR initiators contributed 82% to the CDF. LOCAs contribute the remaining 18%. Loss of RHR from fire, flood, and seismic events accounts for 21% of the CDF, leaving approximately 60% from internal events.

Hardware failure and loss of suction (human induced) are the most important contributors to RHR failure. The importance of the hardware failure of an operating RHR pump results from its long mission time. The importance of the loss of RHR suction results from either inadvertent closure of the RHR suction valves or low-level cavitation when the reactor coolant system (RCS) was drained–both caused by human error.

Plant operational states with low water level and vented reactor coolant system are more risk significant. About 71% of the total CDF occurred with the RCS vented and partially drained.

Equipment hatch integrity is the dominant factor in early health risks. While LOCAs contribute only 18% to the total CDF, they occur during states where the RCS is filled. Given that equipment hatch integrity is not required when the RCS is filled–it is required during reduced inventory conditions–and that operators have only a short time to restore core cooling because of the LOCA, the study found that it was unlikely that the equipment hatch could be closed before the containment became uninhabitable; thus, LOCAs dominate early health risk.

<u>Safety Assessment of BWR Risk During Shutdown Operations (NSAC-175)</u>

The NSAC-175 study (Ref. 2.13) used a simplified probabilistic analysis approach that considered the dominant failure mechanisms associated with shutdown conditions (e.g., since divisional equipment unavailability dominates random hardware failures, system fault tree models were limited to basic events representing an entire front line system division) to analyze a plant-specific outage. From this analysis, the following perspectives were identified.

Risk (i.e., CDF) from shutdown operations is comparable to full power risk. Core damage frequency for the refueling outage is approximately 4E-6 per year, slightly more than 20% of the approximately 2E-5 Grand Gulf IPE mean core damage frequency for power operations.

Loss of inventory events (i.e., LOCAs and draindowns) are the dominant contributors to CDF risk. LOCAs (medium and large) and draindowns contribute 95% to the core damage frequency, with LOCAs contributing about 90%. The other initiating events (decay heat removal pump failure and loss of AC power) contribute to the remaining 5%. The major contributor to the importance of LOCAs is the water level status of the upper containment pool and the suppression pool. If the upper containment pool is drained completely and the suppression pool is partially drained concurrently, very little water is available inside containment, introducing a vulnerability to LOCAs.

<u>Analysis of Boron Dilution Events at Millstone Unit 3</u>

Probabilistic risk assessment techniques were used to evaluate boron dilution events during modes 3, 4, 5, and 6 (hot standby, hot shutdown, cold shutdown, and refuel) at Millstone Unit 3 (Ref. 2.14). A systematic approach was used to identify the potential dilution flow paths leading to a boron dilution initiating event. Each initiating event was then analyzed using event tree and fault tree technology to determine the frequency of loss of shutdown margin sequences. From this analysis, the following perspective was identified.

Human error is the dominant contributor to the initiating events and the primary characteristic of the plant state (cold shutdown) most susceptible to boron dilution . Human error associated with the primary grade water and component cooling water (the only credible unborated water sources capable of entering the reactor coolant system) was responsible for 60% of the initiating events. Mode 5 (cold shutdown) was found to be the most susceptible to boron dilution events because of the relatively high initiating event frequency assumed for the operator error of failing to divert demineralizer flow during resin flushing operations.

A Risk Assessment of Refueling Outage at Monticello Using a Simple Method

A paper by Rohrer and Nierode (Ref. 2.15) discusses a PRA method used to:

- examine planned outage activities to ensure they pose no excessive risk of boiling or fuel damage (assumed to occur when the fuel is uncovered) either in the reactor or the fuel pool,
- identify higher risk periods and important equipment so that recommendations could be made to manage the risk, and
- provide the capability of quickly determining the risk impact of emergent work and changes to the outage schedule.

From this analysis, the following perspective was identified.

Fuel damage frequency varies with the plant's configuration (i.e. water inventory and equipment status) and decay heat load. The analysis found that the fuel damage frequencies for two adjacent time segments that differ mainly by the water inventory available as a heat sink were about a factor of 10 different, with the larger water inventory time segment having the smaller fuel damage frequency. In addition, the analysis found that the fuel damage frequencies for two adjacent time segments differing mainly by equipment status were about a factor of 10 different, with the time segment having more equipment out showing a larger fuel damage frequency. Finally, the analysis found that the fuel damage frequency for a time segment at the beginning of an outage was about a factor of 10 more than the fuel damage frequency for a time segment at the end of an outage (with the same equipment and water inventory status), indicating that decay heat load is an important factor in determining fuel damage frequency.

Evaluating Transition Risk

A paper by Finnicum et al. (Ref. 2.16) describes a ABB CENO and CE Owners Group method for evaluating the risk associated with transitioning a plant from full power to plant shutdown (not including cold shutdown) to effect repairs, then return to power. A trial application of the methodology by two CEOG utilities for a four-day outage, assuming one high-pressure injection system train was out of service for corrective maintenance, was performed. From this application, the following perspective was identified.

Transition risk is comparable to the risk experienced while staying at full power with the equipment unavailable. The transition risk for Fort Calhoun Station (1.38E-6) and Millstone 2 (2.44E-6) is comparable to the at-power risk (1.61E-6 and 3.85E-6 for Fort Calhoun and Millstone, respectively) where the high-pressure injection train is unavailable for the four-day period.

2.4 International LPSD Studies

LPSD risk studies have been performed for international nuclear power plants (References 2.17 - 2.22). Table 2.6 provides a summary of the perspectives from a review of these studies, with more detail provided in the following paragraphs.

Table 2.6 Summary of perspectives on LPSD risk from international studies.

- Core damage (or fuel damage) risk during shutdown is comparable with the risk associated from full power operations.
- Public risk from events during shutdown can be important.
- Internal fire and flood and seismic-initiated events can be important contributors to shutdown risk.
- Plant operational states with reduced water inventory and/or high decay heat are the more risk-significant states.
- Initiating events that have been analyzed for full power conditions must be reexamined to ensure that all LPSD effects are considered (e.g., reactivity insertions).
- Outages other than for refueling may be important contributors to risk.

Core damage (or fuel damage) risk during shutdown is comparable with the risk associated from full power operations. The French shutdown PRAs for the 900 MWe (Ref. 2.17) and 1300 MWe (Ref. 2.18) PWRs found that risk (i.e., CDF) during shutdown is approximately 50% and approximately 225% the risk from full power operation, respectively. Three other PWR analyses, Sizewell B (United Kingdom) (Ref. 2.19), Gösgen (Switzerland) (Ref. 2.20), and Borssele (Netherlands) (Ref. 2.21) found that shutdown risk was 150%, approximately 95%, and approximately 55% the risk from full power operation, respectively. One BWR shutdown analysis, Mühleberg (Ref. 2.22), found the risk at shutdown to be 25% of the risk at full power.

Public risk from events during shutdown can be important. The Sizewell B Level 3 analysis found that faults at shutdown contributed 43% to the total individual risk.

Internal fire and flood and seismic-initiated events can be important contributors to shutdown risk. Generally, those plants that examined these events found one or more of them to be significant contributors to shutdown risk. The Sizewell study found that internal fires contributed approximately 30% of the shutdown risk while the seismic events contributed 10%. In the Gösgen analysis, approximately 30% of the risk came from internal fire events–internal flood and seismic events were insignificant contributors. The Mühleberg analysis found that about 55% of the shutdown risk came from a combination of internal fire and flood and seismic events. The Borssele analysis found that about 30% of the shutdown risk came from internal fire events.

Plant operational states with reduced water inventory and/or high decay heat are the more risk significant states. The Borssele analysis found that about 85% of the shutdown risk came from the mid-loop (early and late) operational states.

Initiating events that have been analyzed for full power conditions must be reexamined to ensure that all LPSD effects are considered. A reactivity accident scenario that may occur during plant startup was found to have a very high core damage frequency (Ref. 2.23) and Reference 2.17) during a LPSD analysis. In this scenario, a loss of offsite power (the initiating event) occurs when deboration is in progress, causing the reactor coolant pumps to trip. The injection of unborated water continues because the charging pump is supported by the emergency diesel generator. In the analyses, it was assumed that the unborated water would remain unmixed with the reactor coolant and form a slug that is ultimately injected into the core when offsite power is recovered and the operator restarted the reactor coolant pumps. The increase in reactivity would cause fuel damage and challenge the reactor coolant system integrity. This type of accident was found to contribute about 20% of the total fuel damage frequency at shutdown for the Sizewell B facility. Boron dilution was also identified as an issue of concern by the International Atomic Energy Agency (Ref. 2.24).

Outages other than for refueling may be important contributors to risk. In the Gösgen analysis, the risk contribution of outages other than refueling were examined, and it was found that these outages contributed approximately 15% to the total fuel damage frequency at shutdown.

REFERENCES

2.1 D. W. Whitehead et al., “Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1: Summary of Results,” NUREG/CR-6143, SAND93-2440, Vol. 1, Sandia National Laboratories, Albuquerque, NM, July 1995.

2.2 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, Vols. 1-6, Brookhaven National Laboratory, 1994.

2.3 T. L. Chu et al., “Improved Reliability of Residual Heat Removal Capability in PWRs as Related to Resolution of Generic Issue 99,” NUREG/CR-5015, BNL-NUREG-52121, Brookhaven National Laboratories, May 1988.

2.4 U.S. Nuclear Regulatory Commission, “Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance, Part 1, Final Summary Report,” NUREG-1560, Vol. 1, December 1997.

2.5 P. Lobner, W. Horton, and B. Kirstein, “A Preliminary Assessment of Core Melt Probability In Cold Shutdown Following a Postulated LOCA at the Sequoyah Nuclear Plant,” ASI01382-147LJ, Rev. 1, Science Application International, July 16, 1982.

2.6 T. Mankamo, I.S. Kim, P.K. Samanta, “Technical Specification Action Statements Requiring Shutdown, A Risk Perspective with application to the RHR/SSW Systems of a BWR,” NUREG/CR-5995, November 1993.

2.7 T. Mankamo, I.S. Kim, P.K. Samanta, J.W. Yang, S. Gibelli, and W. He, “Action Requirements for AFW System Failures: An Analysis for Four Nuclear Power Plants,” draft, NUREG/CR-6502.

2.8 T. A. Wheeler, D. W. Whitehead, and E. Lois, “Summary of Information Presented at an NRC-Sponsored Low-Power Shutdown Public Workshop April 27, 1999 Rockville, Maryland,” SAND99-1815, Sandia National Laboratories, July, 1999.

2.9 D. C. Bley et al., “Zion Nuclear Plant Residual Heat Removal PRA,” NSAC-84, Nuclear Safety Analysis Center, July 1983.

2.10 Pickard, Lowe, and Garrick, Inc., Westinghouse Electric Corporation, and Fauske & Associates, Inc., “Zion Probabilistic Safety Study,” September 1981.

2.11 J. H. Holderness et al., “Brunswick Decay Heat Removal Probabilistic Safety Study,” NSAC-83, Nuclear Safety Analysis Center, October 1985.

2.12 K. L. Kiper et al., “Seabrook Station Probabilistic Safety Study Shutdown (Modes 4, 5, and 6),” New Hampshire Yankee, May 1988.

2.13 J. R. Hewitt, J. P. Gaertner, and E. T. Burns, “Safety Assessment of BWR Risk During Shutdown Operations,” NSAC-175 Interim Report, Draft Report (Revision 1), Nuclear Safety Analysis Center, December 1991.

2.14 R. L. Beveridge, “A Probabilistic Safety Analysis of Boron Dilution Events at Millstone Unit 3,” *Proceedings: International Topical Meeting on Probabilistic Safety Methods and Applications, 24 Feb.-1 March, 1985*, San Francisco, CA, USA, EPRI NP-3912-SR, p.166/1-9, vol. 3, 1985.

2.15 R.J. Rohrer and C.F. Nierode, “Simple Method for Risk Assessment of Nuclear Power Plant Refueling Outages,” *Nuclear Engineering and Design*, Vol. 167, p 193-201, 1996.

2.16 D. Finnicum et al., “A Methodology for Evaluation of Transition Risk,” *Proceedings on the International Topical Meeting on Probabilistic Safety Assessment PSA ‘96 - Moving Toward Risk Based Regulation, 29 Sept - 3 Oct, 1996,* Park City, UT, p 100-105, 1996.

2.17 J. M. Lanore, “The French 900 MWe PWR PSA Results and Specificities,” *Proceedings of the CSNI Workshop on PSA Applications and Limitations, September 4 – 6, 1990, Santa Fe, New Mexico*, NUREG/CP-0115, SAND90-2797, p 75-80, February 1991.

2.18 F. Montagnon, “Probabilistic Evaluation of Risk During Shutdown,” *Proceedings of an IAEA technical committee meeting on modeling of accident sequences during shutdown and low power conditions, 30 Nov – 3 Dec, 1992, Stockholm (Sweden)*, International Atomic Energy Agency, Vienna (Austria), IAEA-TECDOC-751, p 51-55, June 1994.

2.19 M. L. Ang, A. K. Brook, and D. B. Utton, “A Shutdown Probabilistic Safety Assessment for Sisewell B Nuclear Power Plant,” SVA Further Education Course on Safety of Nuclear Power Plants during Shutdown, March 29-31, 1995.

2.20 Shobha B. Rao, and Jürg Landolt, “A Results of the Gösgen Level 1 PSA for Nonfull-Power Conditions,” Technical Committee Meeting, IAEA, Arnhem, Netherlands, November 8-11, 1994.

2.21 M. van der Borst and J. Julius, “Finalization Borssele PSA Projects Part II: Results,” PSA-3 Results, March 1995.

2.22 R. Summitt, A. Torri, and D. Haschke, “Development of a Full-Scope Shutdown PSA For The Mühleberg Nuclear Power Plant,” *Proceedings on the International Topical Meeting on Probabilistic Safety Assessment PSA ‘96 - Moving Toward Risk-Based Regulation*, Park City, Utah, September 29 – October 3, 1996, p 93-99, 1996.

2.23 Teller, N., "The Use of P.S.A. Results in France by Safety Authorities," *Proceedings of the CSNI Workshop on PSA Applications and Limitations, September 4 – 6, 1990, Santa Fe, New Mexico*, NUREG/CP-0115, SAND90-2797, p 159 - 164, February 1991.

2.24 IAEA, “Safety Analysis of Nuclear Power Plants During Low Power and Shutdown Conditions,” IAEA-TECDOC-1042, International Atomic Energy Agency, Vienna, Austria, 1998.

3. CURRENT METHODS AND TOOLS FOR LOW POWER AND SHUTDOWN RISK

This section provides perspectives on low power and shutdown (LPSD) methods and tools developed in the United States (U.S.) and currently available. Only those methods and tools surveyed by the Nuclear Regulatory Commission (NRC) for the purpose of developing an understanding sufficient to support risk-informed regulatory decision-making are discussed below[7]. The scope, approach, level of detail, and principal use of these methods and tools are discussed here. The adequacy of the methods and tools is addressed in Section 4. Overall perspectives are summarized in Table 3.1.

Table 3.1 Perspectives of Low Power and Shutdown Risk Methods and Tools

- Most of the industry methods and tools were developed for configuration risk management (CRM) purposes.
- CRM is primarily performed using qualitative defense-in-depth approaches using NUMARC 91-06 (Nuclear Management and Resources Council) guidelines (Ref. 2.41.
- Probabilistic risk assessment (PRA) is used for CRM purposes to augment defense in depth by more than one half of the U.S. utilities.
- LPSD PRA risk models typically cover refueling outages only.
- The scope of an LPSD PRA typically is an accident analysis for internal events (excluding fires and floods) during cold shutdown and refueling operational states.
- Risk measure metrics include boiling frequency, core damage frequency, and fuel damage frequency.
- Few LPSD PRAs include an accident progression or consequence analysis.
- In principle, the software tools available for LPSD risk analysis can be used to develop a model with any desired level of detail or breadth of scope.

Perspectives on the various LPSD PRA methods are provided in Section 3.1. The contrasts between traditional Level 1 PRA methods and methods for CRM are provided in Section 3.1. Perspectives on the various tools developed by industry for qualitative and quantitative CRM are provided in Section 3.2.

3.1 LPSD PRA Methods

Two approaches can be used to develop an LPSD Level 1 model. One approach is to start with a full-power Level 1 model (if available) and modify it for LPSD conditions. A second approach is to develop an LPSD model independent of any full-power model.

Regardless of which model development approach is used, two different “cases” can be represented by the LPSD model: 1) a traditional time-averaged PRA model, similar in structure to full power PRAs, or 2) an outage-specific model.

Typically, PRA applications to LPSD have focused on particular outage types and on specific plant operational states within these outage types. Examples of this type of approach

[7] This survey was not exhaustive. Other methods and tools may exist which are not included in the present survey.

are the NRC LPSD PRAs of the Grand Gulf (Ref. 2.2) and Surry (Ref. 2.3) plants. In the Surry study, both refueling outages and drained maintenance outages were analyzed, while only refueling outages were analyzed in the Grand Gulf study. Both studies involved two phases. Phase 1 was a rough Level-1 screening study of all plant operational states, while phase 2 consisted of a detailed Level-3 internal event analysis of selected plant operational states, excluding internal fire and flood scenarios. Phase 2 of the Surry study considered mid-loop operation, while phase 2 of the Grand Gulf study considered cold shutdown conditions. A typical CRM model considers cold shutdown and refueling modes of a refueling outage. Some traditional LPSD PRA applications have covered planned and forced outages in addition to refueling outages to get a comprehensive risk profile. An example of this is the industry study of the G sgen (Ref. 2.4) plant in Switzerland.

A shutdown PRA model is developed for each plant operational state (POS) and an associated core damage frequency (CDF) is calculated. An outage is divided into plant operational states (POSs) on the basis of reactor coolant system (RCS) level, temperature, pressure, decay heat load, and potentially other parameters. For example, in the NRC-sponsored Surry LPSD PRA, 15 POSs were defined for a refueling outage based on the power level, RCS level, temperature, and pressure, whether or not the vessel head is off, and whether the containment is open or closed. POSs for other outage types were fewer in number but were defined in a similar way. In the Safety Monitor (Ref. 2.5) models for CRM, POSs are subdivided further into configurations based on equipment availability and, each plant configuration during a POS is examined individually. Some CRM models (Ref. 2.6) (Ref. 2.7) developed using outage risk assessment and management (ORAM) and equipment out of service (EOOS) do not explicitly define POSs. Instead they evaluate a large number of configurations that are defined by the outage schedule. Other CRM models (Ref. 2.8) define POSs in the same way Safety Monitor models define them.

The typical scope of an LPSD PRA includes an accident analysis for internal events only. Three categories of initiating events are analyzed; loss of shutdown heat removal, loss of RCS inventory, and loss-of-coolant accidents (LOCAs). When the fuel is off-loaded to the spent fuel pool, loss of pool cooling is considered.

3.1.1 Level 1 Methods

Perspectives regarding development of an LPSD Level 1 model are discussed below. The differences between the traditional “time average” PRA approach and the CRM approach are highlighted in 3.1.1.1, adaptation of full power model is examined in 3.1.1.2, and the various elements of an LPSD Level 1 model are discussed in 3.1.1.3.

3.1.1.1 Traditional PRA or “Time Average” Approach Versus Outage Configuration Risk Management

The objective of a traditional LPSD PRA is to assess the risks associated with the LPSD operations and identify the important contributors to the risks, while the objective of a shutdown CRM is to evaluate outage plans in order to identify and avoid high-risk configurations. A traditional LPSD PRA performs a PRA for each of the POSs using an approach similar to that of a full-power PRA. The results of the traditional PRA can be added to that of the full-power PRA to obtain a total risk of the plant. The CRM objective can be accomplished qualitatively or quantitatively. The defense-in-depth concept of NUMARC 91-06 is the qualitative approach widely used in the U.S. industry. The objectives of the qualitative defense-in-depth CRM approach are to (1) provide systems, structures, and components (SSCs) to ensure backup of key safety functions using redundant, alternate, or diverse methods; (2) plan and schedule outage activities in a manner that optimizes safety system availability; and (3) provide administrative controls that support and/or supplement the above elements. Utilities implement this concept by developing defense-in-depth worksheets that specify the SSCs that can be used to perform the safety functions, and by developing contingency plans that maintain defense-in-depth by alternate means when pre-outage planning reveals that the specified SSCs will be unavailable. The quantitative approach performs a PRA for each of the configurations at shutdown, conditional on the equipment available and the time the plant spent in the configuration. The results can be plotted as a function of the time throughout the outage and used to identify the high-risk configurations.

The output from an LPSD PRA model that provides an average CDF can be compared directly to a traditional full-power CDF. In this approach, past outage experience is used to calculate the frequency of a baseline outage. Averaged parameters are used to estimate the duration of each POS and to estimate equipment failures and unavailabilities within a POS. The CDFs associated with each POS are directly summed to calculate an "average" CDF on a per-year basis. Therefore, the resulting LPSD CDF can be directly compared to the "average" CDF on a per- year basis typically calculated in full power PRAs[8]. The LPSD CDF can also be directly added to the full-power CDF to calculate a total CDF that includes the contribution from full power as well as low power and shutdown operations.

The output from an LPSD model that provides a CDF for a particular (i.e., unique) outage, as is done in the quantitative CRM approach, cannot be *directly* compared to a traditional full power CDF. With the CRM approach, a conditional CDF is calculated for each specific (i.e., unique) POS within the outage, which represents the risk conditional on being in that POS. The outage plan being evaluated defines the configurations that the plant is in, specifies exactly what equipment is out of service in a configuration, and specifies exactly how long the configuration will last. The PRA model, which typically uses boiling frequency, core damage frequency, and fuel damage frequency as the metrics for evaluating the outage plan, calculates these metrics conditional on the plant being in the specified configuration. The equipment failure data used are either generic or plant-specific, but the equipment unavailabilities are actual and reflect the actual plant schedule for that particular outage. The CDF (or other risk metric) of each POS is multiplied by the actual duration of the POS to obtain a core damage probability (CDP) of the POS. By summing these CDPs, a cumulative CDP associated with that specific outage is obtained. This cumulative CDP could be multiplied by an outage frequency to obtain a CDF contribution of this particular outage. It has been the opinion of much of the industry that every refueling outage is different and no baseline outage exists. Therefore, the average over a few outages would have to be calculated in order to obtain an average CDF that is *directly* comparable to the one estimated with the "time average" method.

The specific industry tools developed for CRM and their unique features are discussed in Section 3.2.

3.1.1.2 Adaptation of Full Power Model

An LPSD Level 1 PRA models can be developed from "scratch" or adapted from a full-power PRA. Although LPSD PRA models can be built from the ground up, analysts typically take advantage of existing PRAs for full power conditions, since there is a long history of full-power PRAs at many plants.

Full-power PRA models can be modified for certain LPSD plant modes where the RCS

[8] Technically, the ful- power CDF assumes that the plant is in that configuration for one year; thus, one should not compare the numbers directly. However, since the average fraction of time the plant is at full power is very near 1.0, making the comparison directly does not necessarily introduce a significant error. Nevertheless, to be correct, the full-power CDF should be adjusted by the fraction of time the plant is at full-power during a year.

temperature and pressure are similar to those at full power. The RCS temperature and pressure for pressurized water reactor (PWR) plant modes in which steam generators are used to remove heat from the core (i.e. startup, hot standby, and hot shutdown) and boiling water reactor (BWR) plant modes in which the condenser is used to remove heat from the core (startup and hot shutdown) are similar to those at full power. Therefore, PRA models developed for full power conditions can be adapted. For example, in the Gösgen LPSD PRA, the full-power PRA models were used to model operations from full power down to 0% power during power descent for shutdown, and from 25% to full power during power ascension. By appropriately modifying full-power PRA models for success criteria, system configuration, and end states, a model was developed for the conditions after 0% power is reached, but prior to the initiation of residual heat removal (RHR), and after RHR is terminated, but before 25% power is reached.

When full power models are used, modifications to account for the unique conditions during LPSD are made. Because a plant undergoes several transitions during shutdown, it may be necessary to estimate the frequency of some initiating events separately for each plant operational state. For example, the frequency for some initiating events may be higher than those for a PRA with the reactor at full power because of the increased level of human activity during shutdown. The availability of safety features is also reexamined. For example, full-power fault tree models are modified to reflect unavailability of automatic actuation of safety systems. A realistic model also accounts for the appropriate decay heat level when the accident occurs.

When a plant's RHR system is being used to remove decay heat, conditions differ significantly from those of full power operation, and the LPSD PRA model becomes significantly different from that of power operation. To account for the shutdown conditions, shutdown-specific initiating events have to be defined and shutdown-specific event trees have to be developed. Section 3.1.1.3 discuss these analyses in more detail.

In the case of system fault trees, if the full-power model is used as the starting point, it is reviewed and modified to represent the system alignment during LPSD conditions. For example, the normal position of a valve during LPSD may be different from that of power operation. Often, new fault trees are developed for systems that are not modeled in the full-power PRA, such as the reactor water cleanup system of a BWR.

Since plant operation during LPSD states requires continuous operator action, human reliability analysis becomes even more important for modeling shutdown than for full power. When human reliability analysis (HRA) methods developed for power operations are modified for application to LPSD conditions, the differing response time periods and other unique aspects of operations during LPSD are taken into account.

3.1.1.3 Elements of an LPSD PRA Level 1 Model

A Level 1 LPSD PRA includes the same elements as a full-power PRA. Regardless of what plant conditions are analyzed, a PRA analyst must perform the same tasks: identify initiating events, identify success criteria, develop the accident sequences (event trees), develop system models (fault trees), estimate failure probabilities (including common-cause), select a suitable HRA method and appropriate human error data, perform the quantification to estimate a CDF (or other risk metric) , and interpret the results. These iterative steps are the same for both full-power and LPSD conditions.

For the most part, the discussion below applies to both the traditional and CRM methods. As indicated above, the CRM methods are different with regard to data needs. Other differences involve the fault tree logic and level of detail used in some CRM methods. These aspects are discussed for the individual CRM tools in Section 3.2.

Initiating Event Analysis

The method for performing an LPSD PRA initiating event analysis is the same as that of a full-power PRA. It includes identification, categorization, and quantification of initiating events applicable to the LPSD conditions. An initiating event is typically defined as an event that causes interruption of the decay heat removal, a loss of RCS inventory, or a reactivity accident. Typically, plant-specific data as well as generic data is collected and used in estimating initiating event frequencies. The scope of a particular study determines the range of events considered.

Accident Sequences and Success Criteria

LPSD event trees are developed by reviewing plant-specific abnormal procedures for shutdown and emergency procedures for power operations, performing supporting thermal hydraulic calculations, and carrying out discussions with plant personnel. Such a process is needed because the strategies for mitigating shutdown accidents are not always clearly specified in procedures. Typically, a plant has a procedure for loss of decay heat removal, and the strategies in the procedure are backed by engineering calculations. The procedure is used in developing the event trees for loss of decay heat removal and loss of support systems. For a loss of inventory event, either the loss of decay heat removal procedure or a separate loss of inventory procedure, if available, is used.

Typically, to determine success criteria and timing of accidents, e.g., time to core uncovery and time to low pressure injection pump shut off, simple computer programs based on energy and mass balances are written. They take into account decay heat level, core inventory, RCS temperature, pressure and level, whether the RCS is vented or open, and the status of the RCS relief valves. More sophisticated codes are used as well. For example, in the NRC study for Surry, the success criteria gravity injection from the refueling water storage tank (RWST) was determined using the MELCOR (Ref. 3.9) code. For the success criteria of reflux cooling, results from Westinghouse (Ref. 3.10) and Idaho National Engineering Laboratory (Ref. 3.11) (Ref. 3.12) studies were used.

In the NRC-sponsored LPSD PRAs, a "time window" approach based on changing success criteria with decay heat was used. The approach specifies separate success criteria for different outage time windows to account for the varying decay heat level during an outage, producing a more realistic modeling of the scenarios. Accounting for the varying decay heat level allows success criteria to be specified separately for each time window and results in a better model than using enveloping criteria to cover the entire outage.

Systems Analysis

Shutdown-specific system configurations are identified by reviewing operating procedures used during shutdown, shift supervisor's log books, and the system training manuals. Otherwise, an LPSD system analysis is performed in the same manner as that of a full-power PRA. If a full-power PRA is used as the starting point, the full-power fault trees are reviewed and modified for shutdown conditions to reflect shutdown-specific configurations. A few systems not used in the full-power PRA will require the development of new fault trees. Just as for full-power systems analysis, different system analysis methods can be used. For example, the NRC studies used the fault tree linking approach, while the industry study of G sgen used the event tree linking approach.

Data and Common Cause Failure (CCF)

An LPSD-specific data collection and analysis is carried out. In a traditional time-averaged PRA approach, this includes data on frequency of outages, initiating event data, failure rates, and

CCF parameters of additional components and systems modeled for shutdown, maintenance unavailability data, fraction of the time a system or component is in a particular condition (e.g., the fraction of time the pressurizer safety valves are removed), time after shutdown when a POS is reached, and duration of POSs. Typically, the analysis assumes that the hardware failure rates, including common-cause failure parameters, used in a full-power PRA are applicable to shutdown conditions. Engineering judgment will likely be needed to estimate some parameters, such as the probability that the containment sump is plugged due to increased activities inside the containment and the probability that the reactor coolant loops are isolated. The timing information developed supports the quantification of the accident sequences using realistic success criteria and accident timing. In a CRM approach, the frequency of outage is not needed, and the duration of POSs, the fraction of time a system is in a particular configuration, and maintenance unavailabilities are specified by the outage schedule. No data analysis on these parameters is needed.

Human Reliability Analysis

Typically, HRA methods developed for a full-power PRA are used for LPSD conditions. The differences in time available, level of detail of procedures for LPSD versus full-power PRA, and unique LPSD conditions are taken into account when applying one of the available HRA methods. In practice, a number of different HRA methods have been used. For example, the NRC study for Grand Gulf used the Accident Sequence Evaluation Program (ASEP) method, while the NRC study for Surry and the industry G sgen study used the failure likelihood index (FLIP) method.

In some LPSD studies, HRA methods were more fundamentally adapted for LPSD conditions. An example is the Borssele LPSD study (Ref. 3.13) where the EPRI (Electric Power Research Institute) Systematic Human Reliability Procedure (SHARP) framework was used to incorporate the human-hardware interactions during shutdown into the PRA. A similar approach is used with the Safety Monitor CRM tool. The Borssele LPSD study made an attempt to address errors of commission in the model. Its approach includes identification of opportunities for error and failure modes of functions, systems, or components that could arise from such errors; screening of errors; and quantification of errors.

Accident Sequence Quantification

An LPSD PRA is quantified in the same manner as a full-power PRA. In the traditional PRA approach, the sequence frequencies of a POS include the frequency of the outage and the fraction of time that the plant is in the given POS. In the CRM approach, the sequences are quantified conditional on the plant being in the POS, and the sequence frequencies do not include the outage frequency and the fraction of the time plant is in the POS. Quantification tools used for full-power PRAs are used for LPSD also. For example, the SAPHIRE code, which uses the fault tree linking approach, was used in the NRC studies, while the RISKMAN code was used for the industry G sgen study. Truncation limits used can be significantly lower than those typically used in a full-power PRA, due to the small fraction of time that the plant analyzed is in any one POS.

3.1.2 Level 2 Methods

The methods used for LPSD Level 2 studies have been the same ones as those used for full-power PRAs. As with the Level 1 model, an LPSD Level 2 model can be adapted from an existing full-power model or developed independently. In practice, when a Level 2 LPSD analysis has been performed, it has always been based on existing full-power models. No new methods or tools have been developed. The applications of the full-power methods and tools properly accounted for the differences in containment isolation, fission product inventory, and slower progression of release due to reduced decay heat at shutdown. Few level-2 LPSD analyses have been performed for U.S. plants. They include the NRC-sponsored studies of Grand Gulf and Surry, and an industry study of Seabrook. The NRC-sponsored studies used the same approach and tools as those used in NUREG-1150, and the Seabrook LPSD study used the same approach as the full power Seabrook study for Level 2. The Level 2 PRA elements were addressed as follows in the LPSD studies performed.

Plant Damage States

The decay heat level attribute is one of the unique characteristics of LPSD plant damage states analysis. It allows decay heat level to be taken into consideration for the Level 2 analysis. Otherwise, accident sequences are binned into plant damage states in the same manner as for full-power states. Critical attributes for defining individual plant damage states include time window or decay heat level, as well as the status of AC power, RCS status at the onset of core damage, emergency core cooling system status, recirculation spray, and RWST status.

Accident Progression and Containment Performance

The status of the containment and equipment hatch is the event unique to an LPSD accident progression. Containment performance involved principally whether or not the containment and/or equipment hatch were open or closed, and if full pressure capacity was available. Full-power methods adapted to LPSD conditions are used. In the NRC studies, a simple Accident Progression Event Tree (APET) was used, along with the EVNTRE (Ref. 3.14) code, developed for the full-power studies of NUREG-1150, with a reduced and simplified number of questions. Deterministic calculations with MELCOR were performed to obtain the timing of key events in the accident progression. The MELCOR code was also used to evaluate basemat melt-through and containment over-pressurization, and found them not credible due to the lower decay heat level which reduces both the concrete erosion rate as well as the containment pressurization rate from that at full power. The possible lack of spray availability, since some trains were taken out of the plant for service during shutdown, was taken into consideration.

Characterization of Radionuclide Release

Full-power methods are applied, but typically simplified in terms of timing and by the recognition that certain types of releases could not occur for certain power levels. In the NRC studies, a parametric source term code based on the XSOR (Ref. 3.15) method developed for NUREG-1150 was used. However, the code was greatly simplified. Release fractions were based on full-power analysis. In the NRC's Grand Gulf study, there was a preliminary analysis carried out to estimate the behavior of a core in an air atmosphere, i.e. core oxidation in an air rather than steam environment, and modified equations for different source term species and amounts were developed.

3.1.3 Level 3 Methods

The only LPSD studies performed in the U.S. that included a Level-3 analyses are the NRC-sponsored Grand Gulf and Surry LPSD PRAs and the Seabrook shutdown PRA. Full-power methods and tools were used, but the analysts accounted for the differences in containment isolation, fission product inventory, and slower progression of release due to reduced decay heat at shutdown. The NRC LPSD PRAs used the same approach and tools as those used in the NUREG-1150 study, i.e., MELCOR Accident Consequence Code System (MACCS) (Ref. 3.16), to calculate offsite consequences. In the NRC studies, the partition code was set to calculate early and latent health fatalities, but was also reset to account for the fact that at certain time windows radionuclide decay was such that early fatalities could be ruled out. Different partition health weights were assigned for each time window. The MACCS code was run with the same risk measures used in the NUREG-1150 study: early fatalities, latent fatalities, and person rem. In addition, an onsite or "parking lot" dose rate was estimated based on a combination of models by Wilson (Ref. 3.17) and those in Regulatory Guide 1.145. The same methodology to propagate uncertainty as that used in NUREG-1150 was used throughout the NRC LPSD studies. The consequence model of the Seabrook shutdown PRA was also based on the full-power PRA of that plant.

3.2 Specific Configuration Risk Management Tools

The three software tools surveyed for this report, ORAM (Ref. 3.18) , EOOS (Ref. 3.19) , and Safety Monitor (Ref. 3.20), have been developed or adapted by the U. S. nuclear industry for outage configuration risk management. The objective of the CRM tools is to evaluate the risk significance of the plant configurations defined in outage schedules and to use the results in support of schedule revisions to manage the risk. The tools all interface with outage planning software and thus automate the evaluation of the outage plan. Each tool includes a qualitative and a quantitative capability[9]. The qualitative module facilitates the defense-in-depth approach to outage configuration management, while the quantitative module is used for a probabilistic safety assessment approach. The metrics calculated by the quantitative module include core damage frequency, time to boiling, and boiling frequency. If fuel is off-loaded from the core, the tools can also calculate the fuel damage frequency of the fuel in the spent fuel pool.

The CRM tools developed for outage management typically have been applied for refueling outages only. The CRM tools were applied toward optimizing refueling outages while preserving adequate margins of safety, not for calculating overall outage risk. However, there are no inherent limitations in the tools to prevent their application to a wider range of outages in the future.

The qualitative defense-in-depth module evaluates a refueling outage in terms of the ability of the plant to perform the necessary safety functions, e.g., decay heat removal, inventory control, power availability, reactivity control, and containment. The CRM tools facilitate the assessment of the status of the functions for each plant configuration in the outage schedule. The goal of the evaluation process is to alert the plant personnel to cautionary or risky configurations during the outage. Licensees establish controls to limit such configurations. Although the details are different for ORAM and EOOS, they both use a color scheme to indicate safe, cautionary, or risky configurations. For each tool, the licensees choose their own criteria to establish what constitutes a transition from safe to cautionary, and from cautionary to risky.

The PRA part of the tools can support CRM of all modes of plant operation. The user determines the scope, level of detail, and end states to be included in the model. The tools themselves are not limited to certain modes of plant operation. EOOS and Safety Monitor were originally developed for configuration management during power operation and then adapted for LPSD CRM, while ORAM was originally developed for shutdown conditions and then extended to power operation.

All three tools are able to quickly quantify the conditional risk profile of a particular outage. Typically, an outage is divided into a few POSs or phases, plant states, and configurations. The terminology has not been standardized. A PRA model is developed for each POS taking into consideration the specific plant conditions and decay heat level. The PRA models can be quantified conditional on the maintenance unavailabilities specified in the outage plan. A plot of the conditional core damage frequency throughout the outage is the risk profile of the outage. All three tools allow fast evaluation of the variations of an outage plan to achieve a safe and efficient outage. This is achieved by the enhanced capability of personal computers, efficient software algorithms, and efficient setup of the logic models.

[9] A defense-in-depth feature was to be incorporated into Safety Monitor by the end of the summer in 1999, but it was not available for review during the site visits for this program.

While these tools have many similarities, each has unique features. A high-level summary of these features is given below.

3.2.1 Outage Risk Assessment and Management

The ORAM approach to system modeling is different from that traditionally used in a PRA. ORAM uses train-level fault trees only to treat system dependencies and not calculate system failure probabilities, as typically done in a PRA. The fault trees are developed independently but are solved within ORAM. System failure probabilities used in sequence quantification are calculated off-line by the analyst's tool of choice. Frequently, system fault trees developed for the plant's Individual Plant Examination are modified for the shutdown condition to calculate hardware failure probabilities needed for evaluating boundary conditions, equipment unavailabilities, and top event failure probabilities.

ORAM apporoach to event tree quantification is different from that traditionally used in a PRA. ORAM uses event trees to define the sequences in terms of success and failure of the top events. However, sequence quantification does not involve linking the fault trees of the top events. The top event failure probabilities are determined by equipment unavailabilities (reflecting the plant's specific configuration being evaluated) and random hardware failures. If the equipment unavailability of a particular plant configuration causes the top event to occur, then the top event has a probability of one. Otherwise, the top event probability is assigned a pre-calculated value, as described above. That is, the pre-calculated values used in the ORAM sequence quantification are obtained by quantifying a fault tree for the top event, taking into consideration the different boundary conditions that may occur.

EOOS is using a single master logic fault tree to represent the accident sequence logic of a PRA. EOOS is a module of the Risk and Reliability (R&R) Workstation (Ref 3.21). Therefore, it interfaces with the PRA models developed using R&R Workstation and is supported by tools available in R&R Workstation to allow fast evaluation of an outage schedule. In order to perform quantification quickly, the EOOS model is in the form of a single large fault tree for the risk metrics of concern, e.g., CDF or boiling frequency. Logic flags are used with the master logic fault tree to remove or incorporate logic for specific plant conditions, boundary conditions, and event sequences.

EOOS also has the option of using pre-generated cutsets. This cut-set approach has the advantage of being faster than regenerating cutsets from a master logic fault tree every time. However, the answer tends to be less accurate, especially for configurations in which many items of equipment are out of service.

EOOS has the interface needed to import PRA models developed with other types of software. Because PRA models typically are not in the form of a single large fault tree, the user has to convert its PRA model into large fault tree model using utility programs supporting EOOS.

3.2.2 Safety Monitor

A single integrated logic model that covers full power and shutdown modes is used in Safety Monitor. With Safety Monitor, a PRA model has to be developed using separate PRA software and then converted into a Safety Monitor model. Safety Monitor was originally developed for online maintenance during power operation and later enhanced to include interfaces with outage planning software, and the capability of modeling all modes of operation. Similar to the EOOS model for shutdown, a Safety Monitor model is in the form of a single large fault tree for CDF or boiling frequency. In the model, the same set of basic events representing hardware failures is used for all modes, and rules of applicability are employed to determine the appropriate parts of the fault tree and basic events that are used in specific accident scenarios. Quantification is performed using the linked fault tree approach for each configuration. The applicable switch settings and event probabilities for the specific condition the plant is in are used.

Safety Monitor uses a generic template of POSs as the starting point for developing plant-specific POSs. Safety monitor has developed generic templates of POSs for refueling outages of both PWRs and BWRs. For cold shutdown of a PWR, six POSs are defined depending on the pressurizer level, RCS level, and whether or not vents in the RCS exist. For refueling operations, three POSs are defined based on the water level in the vessel or refueling basin. Two POSs are used for the spent fuel pool, representing conditions with fuel being transferred and fully off-loaded. The POSs are specialized for an individual plant based on the plant's design and operation. Each POS has its own set of success criteria of the critical safety functions. Within each POS, the equipment out of service may change according to the outage schedule. As a result, the POS is subdivided into plant configurations, and the risk model changes from configuration to configuration.

REFERENCES

3.1 “Guidelines for Industry Action to Assess Shutdown Management,” NUMARC 91-06, December 1991.

3.2 D. Whitehead, et. al., “Evaluation of Potential Severe Accidents during Low Power and Shutdown Operations at Grand Gulf Unit-1," NUREG/CR-6143, Vols. 1-6, Sandia National Laboratory, 1994.

3.3 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, Vols. 1-6, Brookhaven National Laboratory, 1994.

3.4 Shobha B. Rao, and Jürg Landolt, “Results of the Gösgen Level 1 PSA for Nonfull-Power Conditions,” Technical Committee Meeting, IAEA, Arnhem, Netherlands, November 8-11, 1994.

3.5 Jeffrey A. Julius, and Diane M. Jones, “Insights from Developing Shutdown Risk Monitor Models,” International Topical Meeting on Probabilistic Safety Assessment, PSA’99, Washington DC, August 22-26, 1999.

3.6 “Safety Assessment of BWR Risk During Shutdown Operations,” EPRI Outage Risk Assessment and Management (ORAM) Program, NSAC-175L, August 1992.

3.7 “Development of Shutdown Probabilistic Safety Analysis (PSA) /Shutdown Equipment Out of Service (EOOS) for River Bend Station,” EPRI, TR-113084, June 1999.

3.8 “Safety Assessment of Diablo Canyon Risks During Shutdown Operations,” EPRI Outage Risk Assessment and Management (ORAM) Program, NSCA-195L, June 1993.

3.9 Summers, R.M., et.al., "MELCOR 1.8.0: A Computer Code for Nuclear Reactor Severe Accident Source Term and Risk Assessment Analysis," NUREG/CR-5531, Sandia National Laboratories, January, 1991.

3.10 Audreycheck, T.S., et. al.,"Loss of RHRs Cooling while the RCS is partially filled," WCAP - 11916, Westinghouse Electric Corporation, July 1988.

3.11 Naff, S.A., et.al., "Thermal-Hydraulic Processes During Reduced Inventory Operation with Loss of Residual Heat Removal," NUREG/CR-5855, Idaho National Engineering Laboratory, April 1992.

3.12 Wald, L.W., et.al., "Consequence of the Loss of Residual Heat Removal Systems in Pressurized Water Reactors," NUREG/CR-5820, Idaho National Engineering Laboratory, May 1992.

3.13 “Integrated Probabilistic Safety Assessment for the NPP Borssele,” EPZ Netherlands, PSA3-94-1, June 1995.

3.14 J. M. Griesmeyer and L. N. Smith, “A Reference Manual for the Event Progression Analysis Code (EVNTRE),” NUREG/CR-5174, SAND88-1607, Sandia National Laboratories, September 1989.

3.15 Jow, H. N., W. B. Murfin and J. D. Johnson, “XSOR Codes User's Manual,” NUREG/CR-5360, Sandia National Laboratories, December 1989.

3.16 Chanin, D. I., et. al., “MELCOR Accident Analysis Consequence Code System,” Sandia National Laboratories, NUREG/CR-4691, Sandia National Laboratories, SAND86-1562, Vols. 1 - 3, February, 1990.

3.17 Wilson, D. J., “Dilution of Exhaust Gases From Building Surface Vents,” ASHRAE Trans., 83 (Pt. 1), pp. 168-176, 1977.

3.18 Electric Power Research Institute, “ ORAM-SETNINEL^{TM} Software Version 3.3," SW-112894-CD M Palo Alto, California.

3.19 Electric Power Research Institute, “EOOS, A Tool for Risk Awareness," Version 3.0, November, 1999.

3.20 SCIENTECH, INC, “Safety Monitor^{TM} Software Version 2.00 Verification and Validation (V&V)," RZ23AF.05c, Kent, Washington, September 1998.

3.21 Risk and Reliability (R&R) Workstation has been developed by Science Applications International Corporation, under the sponsorship of Electric Power Institute.

4. ABILITY OF METHODS AND TOOLS TO SUPPORT RISK-INFORMED REGULATORY ACTIVITIES

In this Chapter, the ability of current methods and tools to support risk-informed activities is discussed. As shown in Figure 4.1, there are a variety of regulatory activities, such as Regulatory Guide (RG) 1.174, Part 50, events assessment, inspection and enforcement, and maintenance rule, for which low power and shutdown (LPSD) risk information is needed. Consequently, the current methods and tools are discussed here from the perspective of their ability to provide the risk information needed to support these activities (i.e., support risk-informed regulatory decision-making). As discussed in Chapter 2, LPSD risk information relates to:

- risk importance of LPSD (e.g., core damage frequency (CDF) and public health risk),
- types of initiating events that can challenge the plant during LPSD conditions,
- major contributors to LPSD CDF and public health risk (e.g., dominant initiating event frequencies and dominant failures),
- plant operating states contributing to LPSD CDF and public health risk (e.g., hot shutdown), and
- plant design features (e.g., plant layout, removal of barriers during shutdown).

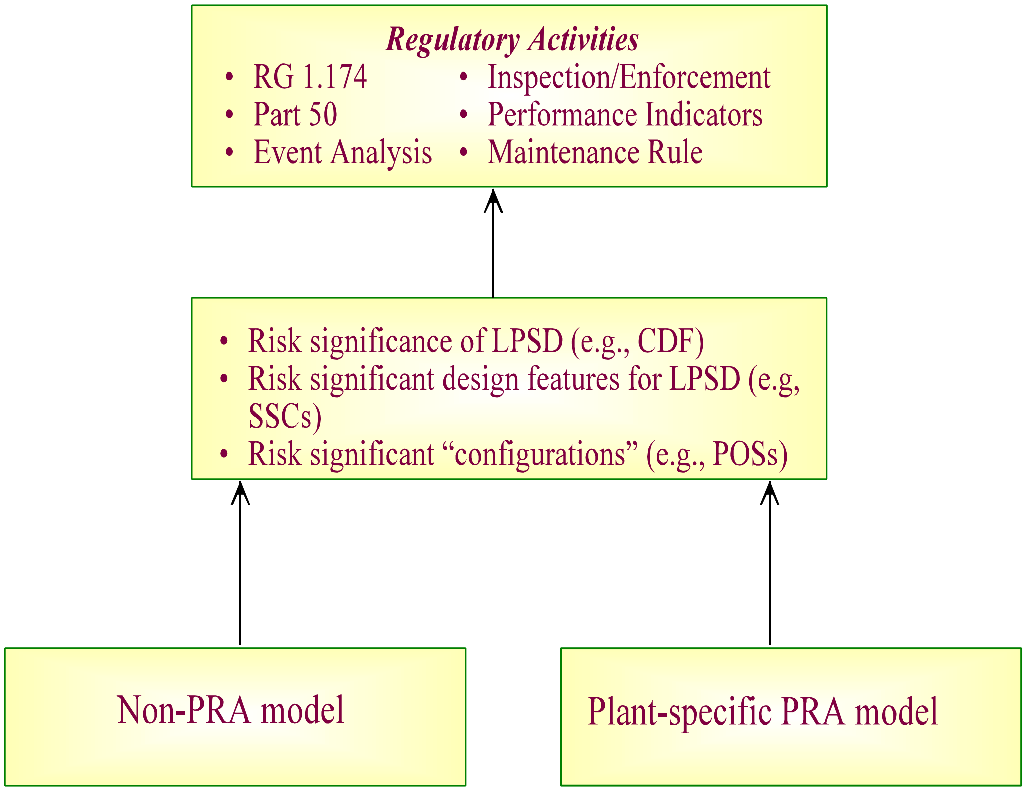

Figure 4.1 Process for incorporating LPSD risk into risk-informed decision-making process.

The type of method employed to provide a technical basis for LPSD risk-informed regulatory activities will depend on the specific issue or the application. Some applications may need a plant-specific probabilistic risk assessment (PRA), while for others, more simplified analyses may be adequate. For the purposes of this report, the "plant-specific PRA approach" is discussed individually; all other approaches are presented as the "non-PRA approach."

These approaches are discussed in more detail in Section 4.1. Section 4.2 discusses the ability of current methods and tools to support the plant-specific PRA , and Section 4.3 does the same for the non-PRA approach.

4.1 Approaches for Incorporating LPSD Risk into Risk-Informed Regulatory Decision-Making Approaches to Perform LPSD PRAs

4.1.1 Plant-Specific PRA Models

This approach requires the development of plant-specific LPSD probabilistic risk assessments (PRAs). These PRAs encompass the whole spectrum LPSD PRAs, ranging from a limited-scope PRA addressing selected plant operational states (e.g., cold shutdown) and selected initiating events (e.g., internal events) to an expanded-scope PRA (e.g., analyzing all operational states for all initiating events).

Current industry LPSD PRAs are typically of limited scope, analyzing:

- planned outages only,
- plant operational states considered most important to outage risk (i.e., reduced water inventory or high decay heat loads during cold shutdown and refueling),
- internal events only (with fire and flood excluded), and
- core performance only (e.g., CDF) (Level 1 analysis); very few LPSD PRAs include an analysis of radioactive releases and their effects on public health (Level 2 and Level 3 analysis).

For some regulatory activities, this type of LPSD analysis may be adequate. However, there may be regulatory activities for which this is not be the case. For example, RG 1.174 requires an assessment of public health risk. For the full-power PRAs, public health risk is incorporated into RG 1.174 through a simplified Level 2 analysis for estimating large early release frequency (LERF). Also, licensees have requested changes in their technical specifications on the basis of external event analyses (e.g., seismic). Therefore, the “plant-specific PRA approach” for regulatory use goes beyond the current practices and includes an analysis of all aspects of LPSD operations, including:

- planned and unplanned outages,
- all LPSD plant operational states,
- all water inventory levels,
- transition between states or configurations,
- spent fuel pool during refueling, and
- all initiating events pertinent to LPSD, including fire, flood, and seismic.

The plant-specific approach involves a Level 1 analysis that includes the above aspects supplemented by a simplified Level 2 analysis to characterize the effects of radioactive releases during LPSD conditions.

The elements of a Level 1 LPSD PRA are:

- Identification of initiating events that could potentially occur during the different LPSD plant operational states (POSs) or configurations (including those not typically seen at full-power analysis, e.g.,loss of shutdown cooling or draindown events),
- Development of event trees for all POSs/configurations modeled,
- Identification of success criteria,
- Development of system models,
- Data analysis, including development of component failure probabilities and common-cause failure (CCF) probabilities,
- Performing human reliability analysis, and
- Quantifying the accident sequences, including performing uncertainty analyses and sensitivity analyses.

The elements of a simplified LPSD Level 2 analysis are:

- Development of plant damage state bins,
- Assessment of credible challenges to the containment,
- Characterization of containment performance limits,
- Probabilistic characterization containment performance, and
- Characterization of radionuclide release.

4.1.2 Non-PRA Approach

There are three aspects to this approach:

- *Qualitative assessments*. For example, the Nuclear Management and Resources Council (NUMARC) in NUMARC 91-06 (Ref. 2.1) has developed guidelines for maintaining defense-in-depth during outages. These guidelines are being used industry wide for configuration risk-management (CRM) during refueling outages. The NRC is also using them for addressing LPSD issues. For example, the NRC is in the process extending the Significance Determination Process, developed to assess the risk significance of inspection findings during full power operations, to cover LPSD. This approach builds on the NUMARC guidelines.

- *LPSD risk information and insights* from existing LPSD PRAs, assessments of operational events, and results from assessments of the risk associated with particular outages derived for CRM purposes. Examples are NRC 's studies related to LPSD issues, discussed in Chapter 2.

- *Simple quantitative evaluations* of LPSD risk, which could be as simple as "engineering judgment," back-of-the-envelope calculations, or more systematic evaluations. For example, questions for LPSD issues are frequently addressed on the basis of full-power models modified for LPSD conditions on the basis of simple back-of-the-envelope calculations. For example, the NRC is in the process of developing simplified PRA models for LPSD operational events.

This approach builds on existing qualitative evaluations, insights, and lessons learned from LPSD studies which include: domestic and international LPSD PRAs, qualitative and quantitative outage assessments, and assessments of operational events. Some key areas of this approach are:

- important initiating events, accident sequences, and contributors;
- safety functions needed to mitigate an event (defense-in-depth);
- plant conditions that could lead to the loss of a safety function (combinations of human and/or equipment failures);
- characteristics of risk-significant POSs (reactor water, decay heat, and pressure levels);
- characteristics of risk-significant plant configurations (e.g., equipment alignment during a specific POS);
- safety function or system success criteria for the different types of initiating events and plant conditions;
- human (operator and procedure) reliability to respond to an accident;
- assessment of credible challenges to the containment;
- characterization of containment performance limits;
- characterization of radionuclide release; and
- sensitivity analyses.

Depending on the application, this information may be used for plant-specific or generic regulatory activities.

4.2 Ability of Methods and Tools to Support Risk-Informed Regulatory Activities Using Plant-Specific PRAs

The strengths and weaknesses of the methods and tools that could be used to perform plant-specific LPSD PRAs to support risk-informed regulatory decision-making are discussed in this section. Methods are discussed in Section 4.2.1 and tools are discussed in Section 4.2.2. Table 4.1 summarizes the weaknesses of the current LPSD practices.

Table 4.1 Summary of limitations of current LPSD practices for application to regulatory risk-informed decision-making.

Initiating Event Analysis • Draindown event causes and frequencies are not well understood. • Limited assessment of internal flood/fire and external events.
Accident Sequence Analysis • Streamlining of accident sequence analysis • Several accident sequences are poorly understood   • spent fuel pool misloading   • cold overpressurization   • crane failure during heavy lifts   • fast-acting reactivity insertions
Success Criteria • Current application of full-power success criteria to LPSD conditions may yield overly simplistic and inaccurate insights regarding risk contributors. • Thermal-hydraulic methods developed for full-power PRA may be inefficient when applied to LPSD condition. • Many LPSD thermal-hydraulic analysis are based on simplistic calculations.
Systems Analysis • Criteria and guidance for modifying full-power system models to match LPSD conditions have not been standardized. • Many utilities express concern that a meaningful baseline LPSD configuration could be defined for risk-informed purposes.
Data Analysis (Component Failure Models and CCF) • Appropriateness of using standby failure data for extended operations is not understood. • LPSD configurations may be significantly different than the basis for which full-power models were developed.
Human Reliability Analysis • Application of full-power recovery models may yield overly simplistic and inaccurate insights regarding risk contributors. • Errors of commission • Transition risk
Accident Sequence Quantification • Only point estimate quantification is performed.
Level 2/3 • No assessment of Level 2 or 3 risk is done. • Source term and release mechanisms relevant to LPSD may not be well understood.

4.2.1 Methods

Level 1 methods used to perform the various PRA tasks are discussed in Section 4.2.1.1. The methods used to perform the tasks associated with a simplified Level 2 analysis are discussed in Section 4.2.1.2. Table 4.2 summarizes the limitations of current LPSD practices that could be used to support risk-informed decision-making.

4.2.1.1 Level 1 Analysis

As stated previously, a Level 1 analysis consists of the following elements:

- Identification of initiating events that could potentially occur during the different LPSD POSs or configurations (including those not typically seen at full-power analysis, e.g.,loss of shutdown cooling or draindown events),
- Development of event trees for all POSs/configurations modeled,
- Identification of success criteria,
- Development of system models,
- Data analysis, including development of component failure probabilities and CCF probabilities,
- Performing human reliability analysis, and
- Quantifying the accident sequences, including performing uncertainty analyses and sensitivity analyses.

Sections 4.2.1.1.1 through 4.2.1.1.7 present strengths and weaknesses for each of these elements.

4.2.1.1.1 Identification of Initiating Events

Strengths

The process by which initiating events are identified for LPSD PRAs is essentially the same as that used for full-power PRAs. Typically, plant systems and operations are examined using various methods (e.g., failure mode and effects analysis, master logic diagrams, examination of procedures, observations of plant personnel activities, etc.) to identify events that could cause an initiating event. These methods have the capability to identify potential initiating events for the different plant power levels and configurations, having been successfully employed for full-power PRAs over many years.

Weaknesses

Unwarranted use of full-power initiating events without appropriately considering LPSD conditions could lead to inappropriate events being identified. For example, identifying loss -of-coolant accidents (LOCAs) as initiating events during shutdown conditions simply because LOCAs are initiating events during full power may be inappropriate if conditions during shutdown (i.e., significantly reduced reactor coolant system pressure) do not provide the mechanism(s) for the event to occur. However, elimination of full-power initiating events must be done with care to prevent the elimination of initiating events for one reason (see above) when new conditions during LPSD (e.g., multiple and/or concurrent maintenance activities) may introduce other ways in which the initiating event can occur.

Screening initiating events (i.e., reducing the number of events to be analyzed to a manageable set) might eliminate some events that would result in core damage before the event is mitigated if the event and its consequences are not fully understood. For example, some screening techniques are based on exceeding some specified recover time (usually estimated from thermal-hydraulic calculations). If the available recover time is greater than 24 hours, the initiating event is screened out. Theoretically, this could lead to ignoring initiating events that require more than 24 hours to correct, even though core damage would not occur during the 24-hour period. Before initiating events are screened, it is imperative that the ramifications associated with such screening be understood.

There is a lack of understanding of how reactor coolant system (RCS) draindown initiating events occur and how LPSD conditions affect the event's frequency of occurrence. Draindown events constitute an important class of initiating events, as discussed in Chapter 2. They typically involve combinations of human and/or hardware failures resulting in reactor coolant drainage from the primary system. Although these events are included in LPSD risk analyses, many experts believe that there is not a good understanding of the causes and the frequencies of these events. Their treatment is simplistic in LPSD PRAs, where the same draindown frequency is used for all plant configurations, although it is believed that draindown frequencies are highly dependent on plant configuration. Furthermore, most analyses are using draindown frequency estimates developed in the early 1990s. Updating the draindown initiating event frequency to include current trends should provide a more accurate representation of the risk associated with this type of currently identified important initiating event. Furthermore, a more systematic examination of the activities performed during LPSD operations, along with associated procedures and controls, will help to better understand the conditions (combination of human and equipment failures) that could result in draindown or other types of initiating events.

Seismic events and internal floods and fires are typically not included in domestic LPSD risk assessments. Many believe that the risk associated with these events is very small and, therefore, can be screened from the analysis. However, as discussed in Chapter 2, the Surry (Ref. 2.2) analysis showed that fire is an important initiator. Also, one licensee, on the basis of its LPSD PRA, was able to show that the most risk significant initiating event for its plant is a seismic event during refueling. The licensee requested a change in the technical specifications for its diesel generators (to perform testing and maintenance with the reactor at power) on the basis of this analysis. This example shows that for risk-informed activities, all initiating events should be considered, including fire, flood, and seismic.

The causal relationships between LPSD plant conditions and internal fire and flood initiators has not been fully investigated. The risk contribution from internal fires and floods has been shown to be important for certain plants, in many cases simply by adjusting the full-power initiating event frequencies to account for events that have happened during shutdown conditions. Such a treatment may result in misleading conclusions if the causal relationships between the plant conditions and the initiating events are not properly understood. Outage activities may present unique challenges to safety with regard to risk from fire and flood by creating opportunities for human-induced fire and flood, which are outside of the scope of random fires and floods typically considered in full-power PRAs. Barriers assumed to be in place for a full-power analysis may have been removed during an outage. The assumptions used to screen flood sources from the analysis at full power may not be appropriate for LPSD. Furthermore, human actions that can initiate a fire or flood, human actions needed to mitigate the initiators, and the plant procedures that control activities during LPSD conditions may need additional examination before the causal relationships can be more fully understood.

4.2.1.1.2 Development of Event Trees for LPSD Conditions

Strengths

Methods for defining and modeling accident sequences in full-power PRAs have been successfully utilized in LPSD risk assessments.

Weaknesses

Some accident sequences related to LPSD conditions are not well understood. The potential significance of some accident sequences may not be well understood due to limitations in knowledge. These sequences included:

- **Spent fuel pool misloadings.** Concern has been expressed by some in industry that the circumstances involved in adding reactor fuel to the spent fuel pool (SFP) and reracking the SFP inventory are becoming increasingly challenging as SFP inventories increase. The management of fuel geometries for SFP reracking is potentially more complex and less well controlled than the geometries for fuel in the reactor. Consequently, there is a concern that the potential exists for a fuel criticality accident in the SFP during a reracking activity. To date, no analysis of potential SFP criticality events has been included in LPSD PRAs.

- **Cold overpressurization.** In the event of a loss of decay heat removal in a pressurized water reactor, the potential exists for a rise in RCS temperature and pressure which could potentially compromise the system's pressure boundary. Previous LPSD analyses on Surry sponsored by the NRC [(Ref. 4.5) and (Ref. 2.3)] have shown that such accident scenarios can be significant contributors to LPSD risk. However, this issue has not been adequately addressed in most industry applications of LPSD PRAs.

  If the RCS is closed at the time of loss of residual heat removal (RHR), then both the pressurizer and the RCS may become solid due to thermal expansion of the coolant, presenting three potential challenges to the primary system:

  - If the power operated relief valves (PORVs) cannot adequately respond to the pressure increase, the RCS pressure boundary could fail.
  - Even if the PORVs successfully relieve the primary system pressure while the pressurizer is solid, the primary system could experience a serious loss of inventory. The PORVs would be emitting liquid coolant directly out of the RCS, and the rate of coolant loss could be much greater than the rate for a static boil-off situation.
  - There exists the danger that the low pressure piping of the RHR system may be compromised by the pressure rise. The RHR system is designed for pressures in the range of 600 psi, and if it is not isolated from the RCS, it could rupture as it is exposed to the RCS pressure during a cold overpressurization event.

  The likelihood and seriousness of this scenario may depend on many plant specific design and operational factors, as well as specific conditions associated with the plant configuration. The relief valve capacity, decay heat level, existence of vents in the RCS, possible interfaces between the primary system and low pressure systems (e.g., RHR isolation status, nozzle dams, and thimble tube seals) are important factors that affect the scenario as well.

- **Crane failure during heavy lifts inside containment.** The potential exists for a serious loss of key safety features should a crane failure or accident occur inside containment during an outage. The risks associated with heavy lift crane failure accidents inside the containment has not been investigated in LPSD PRAs. The general consensus regarding nuclear grade crane failures is that the likelihood of such accidents is low and such accident scenarios are insignificant to risk. However, during the NRC-sponsored workshop on LPSD risk assessment in April, 1999 (Ref. 2.4), it was suggested that the current state-of-knowledge regarding nuclear grade crane failure frequencies is out of date. Current crane failure probabilities (i.e, the drop frequencies for cranes used in nuclear power plants) are based on data which is approximately 20 years old.

- **Fast-acting reactivity insertions.** Fast-acting reactivity insertions (i.e., the rapid insertions of large slugs of un-borated water into the reactor core) represent a potentially dangerous circumstance during outages. This type of event has been identified as a potentially significant risk contributor in LPSD PRAs, but the modeling of such events has been limited. Research conducted by the French suggests that this process may be quite complex.

Event tree models would have to be developed for all plant operating states and all initiating events, including those relevant to unplanned and forced outages. One potential challenge for developing event tree models for unplanned and forced outages would be to comprehensively and efficient model all initial conditions for which accident sequences would have to be modeled.

Streamlining of Accident Sequence analyses. Inherent to LPSD risk analyses is that most plant configurations involve low pressure conditions in the RCS. This has a profound effect on the number of systems which could, in theory, be called upon for injection of coolant into the RCS. The magnitude of the accident sequence analysis could become computationally untenable without a practical approach to screen out systems which are not risk-significant. At the time the NRC's LPSD PRAs on Surry and Grand Gulf were done (Refs. 4.5 and 4.6), this issue was a significant methodological factor in the development of accident sequence event trees. Current industry software tools developed for CRM [i.e., Equipment Out of Service (EOOS) (Ref. 2.5), Outage Risk Assessment and Management (ORAM) (Ref. 2.6), and Safety Monitor (Ref. 2.7)] have been touted as being computationally fast. However, the capacity of these tools to handle full-scope LPSD accident sequence models, as developed in the NRC's Surry and Grand Gulf LPSD PRAs, has not been evaluated.

Streamlining of the accident sequence analysis would not necessarily impact the calculated risk estimate, but rather it would enhance the efficiency of the analysis by allowing the analysts to focus on the more important risk-significant elements of the analysis. There are two facets to the streamlining process:

- identify the more risk-important LPSD conditions and POSs, and
- develop a process that efficiently models the extremely large number of possible unplanned outage states (i.e., the initial event or combination of events that requires the plant to be shutdown and the subsequent response of the plant to all of the accident-initiating events applicable to the shutdown state).

The first part of the streamlining process would be the development of efficient screening methods which might, for example, indicate that for specific conditions (e.g., the reactor cavity is flooded and the upper pools are connected), only a selected set of initiating events (e.g., those that result in the loss of inventory) need to be analyzed in detail because all other initiators can be eliminated due to the significant amount of time (e.g., greater than 24 hours) available to the operators for recovery before fuel damage occurs. In addition, because shutdown risk analyses involve plant configurations with low pressure conditions in the RCS, a practical guideline is needed on how many of the multitude of systems to model (especially for a boiling water reactor) during the accident sequence development phase of the analysis. This guidance must be tempered with the need to allow the risk analysis to be as realistic as possible without causing the analysis to become computationally unacceptable.

The second part of the streamlining process deals with developing guidance to prevent the modeling of large number of entry conditions to unplanned outage states from becoming computationally unacceptable. Guidance in this area might, for example, state that all unplanned outages resulting from failure of *any* component in Train A can be collapsed because *all* component failures have exactly the same effect in the accident sequences.

4.2.1.1.3 Identification of Success Criteria

Strengths

The methods for identifying success criteria, including thermal-hydraulic analytic calculations, developed for full-power PRA, have been successfully applied to LPSD conditions.

Weaknesses

Current application of full-power success criteria to LPSD conditions may yield overly simplistic and inaccurate insights regarding risk contributors. LPSD success criteria for many systems are based on full-power success criteria in lieu of thermal-hydraulic analyses. This practice is especially common for systems that are typically modeled in full-power PRAs. Reliance on full-power success criteria may yield conservatively high and unrealistic risk estimates. In selected cases, the use of full-power success criteria may actually yield non-conservative (or unrealistic) results (e.g., low pressure injection requirements for large loss of coolant events). Such overly simplistic and unrealistic results could lead to misleading and inaccurate insights regarding risk contributors by masking potential contributors to risk.

Thermal-hydraulic methods developed for full-power PRAs may be inefficient when applied to LPSD conditions. Thermal-hydraulic calculations are used in developing success criteria and determining the amount of time that operators have to respond to an event and to recover from component failures. Both response time and recovery time are important attributes to accident sequence analysis, as human actions are one of the most risk-significant classes of events in LPSD analyses. Experience from the NRC's Surry (Ref. 4.5) and Grand Gulf (Ref. 4.6) LPSD PRAs indicate that computer codes developed for full-power thermal-hydraulic analyses can be inefficient when applied to LPSD conditions. Such circumstances can discourage the use of such powerful analytical methods. Consequently, many LPSD thermal-hydraulic analyses are based on simplistic calculations. The resulting analysis may yield conservatively high and unrealistic risk estimates. Such overly simplistic and conservative results could lead to misleading and inaccurate insights regarding risk contributors by masking potential contributors to risk.

Current methods used for relatively detailed thermal-hydraulic calculations, such as MELCOR (Ref. 2.8), should be examined to determine whether they deal efficiently with LPSD conditions.

4.2.1.1.4 Development of System Models

Strengths

LPSD risk assessment can leverage heavily off of models developed for full-power PRAs. Much of the system modeling already done for a full-power PRA can be used as a foundation for the system models for LPSD risk assessment.

Weaknesses

Criteria and guidance for modifying full-power system models to match LPSD conditions have not been standardized. The conversion of existing system models developed for full-power PRAs into LPSD system models has no negative impact on LPSD risk analyses unless done incorrectly. The concept of building on current full-power models to create LPSD models is becoming increasingly popular among risk analysts as they attempt to efficiently use limited resources. Many of the existing full-power system modes can form the foundation of the system models for LPSD risk assessment. However, criteria and guidance for modifying full-power system models to match LPSD conditions have not been standardized. Because LPSD analyses have shown that risk from LPSD conditions can be comparable to full-power risk, it is crucial that full-power system models be thoroughly and systematically reviewed so that they are transformed into accurate LPSD models. Currently, there is no guidance for converting full-power models to LPSD models.

Many utilities express concern that a meaningful baseline LPSD configuration could be defined for risk-informed purposes. If LPSD PRA results are to be used to support risk-informed regulations, a baseline model for LPSD analyses must be developed or defined. This baseline model will provide a mechanism for comparison of the risk resulting from a proposed change. Definition or development of the baseline model should help meet the needs of regulatory decision-making.

Many industry representatives and consultants argued that the spectrum of plant configurations defined across the schedule for planned outages are uniquely different from one outage to the next, making the definition of a baseline configuration difficult. However, several foreign nuclear utilities have defined a baseline outage as a time-averaged configuration (i.e., plant configuration and equipment outages are averaged over some predefined time span). While such an approach has merit, the definition of a baseline configuration must allow for the evolving nature of outages.

4.2.1.1.5 Data Analysis, Including Development of Component Failures and CCF

Strengths

Methods for quantifying component failures and common-cause failures are directly applicable to LPSD conditions.

Weaknesses

The use of standby failure data from full-power PRAs to model equipment that is normally operating during LPSD conditions (e.g., failure rate for standby-pump fails-to-run is used to model the same pump's normally-operating failure modes during LPSD conditions) should be reexamined to determine whether the values are appropriate during extended periods of operation. Past analyses have shown that certain component failures based on failure rates (e.g., diesel generator or motor driven pump fails-to-run for a specified mission time) can be important contributors to risk, especially as the mission time increases. The current practice is to use the same component failure values developed for full-power PRAs in LPSD risk assessments. Such use may be unwarranted, since either or both the operational status and the operational environment for a system and its components at full power can be different than for LPSD conditions. For example, systems that are normally standby for full-power operations can be normally operating during LPSD conditions. The current values used for failure data in dynamic situations (e.g., failure rate used for pump fails- to-run) should be reexamined to determine whether the values are appropriate during extended periods of operation.

The appropriateness of generic full-power common-cause models should be reexamined for the unique conditions experienced during shutdown conditions. System dependencies can be significantly altered through intentional realignments of support systems during outages. Currently, it is a common practice to employ full power common cause failure models in the development of LPSD component failure models. Application of full-power models to LPSD conditions must be done prudently since system configurations can be drastically altered (e.g., compressed air to all diesel generators is switched over to a single supply line during outage, normally standby systems for full-power are normally operating for LPSD conditions).

4.2.1.1.6 Human Reliability Analysis

Strengths

The methods employed to model human reliability analysis (HRA) for LPSD risk assessment are typically the same methods employed for full-power PRA. Methods range from systematic and robust models to simplified time-reliability correlation models.

Weaknesses

In view of the dominance of human related errors in LPSD risk assessments, uncertainties in HRA are a significant technical issue. Issues have been identified regarding three aspects of HRA:

- recovery,
- errors of commission, and
- transition risk.

HRA of recovery actions is an area of uncertainty. Human actions have been identified as one of the dominant contributors to LPSD risk. As such, a more complete understanding of human interactions with plant equipment during LPSD conditions is warranted. One area of uncertainty lies in the use of current HRA techniques to estimate human reliability for LPSD recovery times that frequently extend for many hours (recovery times greater than 24 hours are not unusual). Many industry risk analysts believe that the application of such models to LPSD analyses yield overly conservative results which bound the actual risk. However, this claim has not been validated, and some human reliability analysts believe that the use of full-power HRA models to LPSD conditions may yield overly simplistic and inaccurate risk results which could mask other risk contributors. Furthermore, even if the full-power HRA models only resulted in overly conservative results which bound the actual risk, use of such models could lead to the masking of the truly important risk-dominant factors.

Operator errors of commission are potentially significant for LPSD conditions. LPSD operations, unlike full-power operations, are characterized by numerous dynamic changes to the alignment and state of plant systems and components. Consequently, many operator actions are required throughout an outage, creating the opportunity for a multitude of operator errors of commission. This is an area of HRA that has been identified as challenging to model by industry analysts, and as such has either not been modeled or modeled incompletely in current LPSD risk analyses. The importance of errors-of-commission during LPSD operations has not been well studied or modeled in LPSD risk assessment.

Transition risk, the risk associated with the transition between plant operating modes and between plant configurations, is an area to which limited attention has been given. Currently, there are two meanings to the term “transition risk.” One is rather macroscopic in its risk perspective, and the other more microscopic. The first meaning refers to all of the risk associated with the plant operational modes and POSs involved in the ramping down from full-power to cold shutdown and between cold shutdown and full power during power ascension. The second meaning refers specifically to the risk associated with the realignment of a plant from one configuration to another. The latter meaning does not relate to operations while a plant is in any particular plant mode, POS, or configuration. Rather, it defines the risk associated with the specific operator actions, potential errors of commission, and the potential equipment failures (e.g. pump fails-to-start) involved in transitioning a plant between plant modes, POSs, and configurations.

Risk associated with the transition between full-power and outage modes is inconsistently analyzed in industry LPSD PRAs, being analyzed by some utilities and not by others. The decision to model or not model the risk of transition from full-power to outage modes is a matter of choice with each utility, but LPSD PRA methods are readily capable of handling such analyses. However, such is not the case for the risk of transitioning between plant configurations.

Traditionally, LPSD risk assessments developed for outage CRM have focused on the risk associated with the specific operations undertaken and the system alignments during the duration of each plant configuration, but not necessarily the risk associated with transitioning from one configuration to the next. Like a series of snapshots taken at various time intervals, LPSD risk assessments capture the risk throughout the outage as multiple mini-plant risk assessments, wherein each plant configuration risk is assessed for the specific system alignments and equipment availabilities. Some utilities do not attempt to model the risk of transitioning from one configuration to the next, claiming that the state-of-the-art in errors-of-commission modeling are inadequate to model such issues. Other LPSD risk assessment practitioners attempt to model this risk, but the accuracy and comprehensiveness of their models have not be verified.

As a completeness issue, transition risk could be important, especially since human actions are involved and have been shown to be important in other LPSD analyses.

4.2.1.1.7 Accident Sequence Quantification

Strengths

Quantification methods, including the calculation of importance measures and uncertainty analysis, have been implemented into LPSD risk assessments for time-averaged LPSD PRAs. The methods developed for full-power PRAs, such as Latin Hypercube Sampling (LHS) of basic event probability models and propagation of uncertainty through the Level 1 and 2 models, have been implemented into some LPSD risk assessments.

Weaknesses

The current practice among CRM LPSD risk assessment is to quantify all basic events and accident sequences as point estimate calculations. Techniques and tools used to perform uncertainty analyses have not been incorporated into CRM LPSD risk assessment.

4.2.1.2 Simplified Level 2 Analysis

Adequate consideration has not been given to what a simplified LPSD Level 2 analysis should encompass. Therefore, no method for carrying out a simplified LPSD Level 2 analysis has been generally accepted as adequate or appropriate. A simplified LPSD Level 2 analysis, comparable to that described in NUREG/CR-6595 (Ref. 2.9) for full power operation, was suggested in that report, but has not been used. However, it seems reasonable to expect that a simplified analysis could be developed, which could be used together with a Level 1 analysis for many applications. While it is difficult to discuss strengths and weaknesses of an analysis still to be developed, some general comments are possible regarding the strengths and weaknesses the development of such an analysis would face.

Strengths

The containment performance analysis can likely be adapted in part from simplified full-power methods and augmented with relatively simple containment status checks. For low-power states during which potential core damage accidents can lead to energetic events severe enough to challenge containment, an existing full-power approach can be adapted. For other plant states with power low enough that actual challenges to a closed containment are not credible, a conventional containment performance analysis is not needed, and the emphasis can be on simply determining whether containment is open or closed. Containment analysis would focus on mechanisms for potential containment isolation failure or bypass, as well as the containment status called for by the outage schedule for each plant configuration considered in the analysis.

Weaknesses

There are several major issues which need to be addressed by the formulation of a simplified Level 2 analysis for LPSD. One is establishing what the appropriate Level 2 risk metrics are for LPSD. In previously performed Level 2 LPSD studies, using conventional methods, LERF as well as late releases were calculated. Although LERF is considered by most PRA analysts to be the most important Level 2 risk measure for full-power operation, many LPSD PRA analysts feel that it is not a good Level 2 risk measure for LPSD. However, no other risk measure has been generally agreed on as being more appropriate. Another major problem is the lack of current knowledge regarding the behavior of a degraded core under LPSD conditions. The phenomena that could occur, or the types of fission products which could be released, from an undercooled core exposed to an air atmosphere, as could be the case for some LPSD scenarios, has not been investigated. Not only does this present a serious obstacle to the development of an adequately- detailed Level 2 analysis, it also presents problems for the development of a simplified analysis as well.

4.2.2 Tools

In this section, the strengths and weaknesses of the current tools, ORAM, EOOS, and Safety Monitor are discussed.

4.2.2.1 Level 1 Strengths

Safety Monitor, EOOS, and ORAM are readily capable of supporting a Level 1 PRA approach. These tools are designed to function as platforms that facilitate and automate the manipulation of data and calculations. As such, these tools are capable of accepting input from most types of Level 1 PRA models or analyses to support the execution of the seven Level 1 PRA elements. Most of the supporting models can be either analytically simple or complex.

One of the significant features regarding these tools is that they can accept output from full-power system models. This feature greatly facilitates the development of LPSD system models at the same level of modeling detail as full-power PRA models.

4.2.2.2 Level 1 Weaknesses

Some tools have a limited capability to deal with highly complex models. Specifically, thermal-hydraulic analyses, HRA, and accident sequence quantification are three areas in which EOOS, ORAM, and Safety Monitor may be limited in their capabilities.

Safety Monitor, EOOS, and ORAM have been developed with relatively simplistic capabilities to perform thermal-hydraulic analyses in support of LPSD risk assessment. The primary function of the thermal-hydraulic feature of these tools is time-to-boil calculations. The results of such analyses are used to develop time estimates for input into the accident sequence recovery analysis. These results are also typically utilized to support success criteria development. However, the thermal-hydraulic analytical capabilities of these codes are simple, and may yield unrealistic and potentially misleading results.

With regard to accident sequence quantification, EOOS, Safety Monitor, and ORAM do not currently have the capability to perform parameter uncertainty analysis. Furthermore, there is no capability of calculating risk importance measures with ORAM.

With regard to HRA, tools such as EOOS, Safety Monitor, and ORAM certainly have the capability to accept the results of any type of HRA method. However, the capability of automated incorporation of recovery into accident sequence equations might require modification if simple time reliability correlation recovery models were replaced by more complex HRA models.

4.2.2.3 Simplified Level 2 Strengths and Weaknesses

No Level 2 modeling capabilities have been implemented into Safety Monitor, EOOS, and ORAM.

4.3 Ability of Methods and Tools to Support Risk-Informed Regulatory Activities Using a Non-PRA Approach

The strengths and weaknesses of the current methods and tools that could be used in the three non-PRA approaches to support risk-informed regulatory decision-making are discussed below. Methods are discussed in Section 4.3.1 and tools are discussed in Section 4.3.2.

4.3.1 Methods

The strengths of all three non-PRA approachs are discussed first and then the weaknesses.

Strengths

The LPSD qualitative approach used by the licensees for outage CRM provides a foundation for LPSD qualitative evaluations. The NUMARC 91-06 guidelines focus on the availability of systems, structures, and components (SSCs) so that redundancy and diversity of key safety functions is achieved during outages. The underlying philosophy for defense-in-depth is to plan and schedule outages so that safety system availability is optimized. Guidelines facilitate the identification of plant configurations that could potentially compromise safety during planned outages. A plant's ability to provide key safety functions throughout an outage is achieved by ensuring that redundant and diverse methods for each key safety function are available for all different plant configurations in an outage.

The qualitative approach is widely practiced today and is a well-established method. For example, the NRC's Significance Determination Process for LPSD builds on the NUMARC 91-06 guidelines. This defense-in-depth approach provides a good foundation for developing selected insights regarding LPSD risk that could be useful in some regulatory activities. It could be used for identifying:

- key safety functions needed to respond to an event (defense-in-depth) for the significant POSs/configurations,
- characteristics of risk-significant POSs, and
- characteristics of risk-significant plant configurations (e.g., equipment alignment during a specific POS).

The use of LPSD risk information and insights builds on lessons learned from a broad spectrum of studies. Insights derived from studies of LPSD risk evaluations (including domestic and international LPSD PRAs, assessments of operational events, and PRA outage evaluations performed by licensees for CRM purposes) can be used to develop generic insights regarding the risk significance of the following:

- initiating events,
- accident sequences,
- plant configurations (i.e., equipment alignments and the status of various plant parameters), and
- contributors (e.g., component failures and human actions).

The broad use of PRA by licensees to augment the defense-in-depth approach during refueling outage CRM provides an extensive and increasing set of information from which generic insights can be obtained. Thus, this approach could provide the technical bases for risk-informed regulatory activities requiring generic information (e.g., risk-informing Part 50).

Simple quantitative evaluations are by nature easy to perform, can be performed in a short period of time, and are inexpensive. They range from expert judgment, to "back-of-the-envelope" calculations, to relatively detailed quantitative calculations, and can be used in a wide variety analyses. As such, the strengths depend upon the specific type of simple quantitative evaluation performed. However, they provide a means of quickly obtaining information that may be adequate for the specific type of application.

Weaknesses

The guidelines for LPSD qualitative assessments are implemented on a volunteer basis. Because the NUMARC 91-06 guidelines are implemented on a volunteer basis and are qualitative by nature, certain weaknesses or limitations exist for their use in risk-informed regulatory activities. These weaknesses can be summarized as follows:

- a plant-to-plant variability in the use of defense-in-depth guidelines,
- self-grading by each utility with respect to meeting the defense-in-depth criteria,
- no calculation of a quantitative risk metric,
- no quantitative measure or ranking of the risk significance for each critical LPSD safety function or for deviations from the defense-in-depth criteria,
- no identification of systems or human actions that may initiate an accident,
- no capability to identify which system/component or human action is the most risk-significant,
- no characterization of containment performance limits, and
- no characterization of radionuclide release.

Since the use of LPSD insights builds on insights from other studies, it can have the same types of limitations that the individual studies possess. For example, the limitations discussed for the plant-specific PRA approach in Section 4.2.2 may be applicable to this approach. Furthermore, extensive effort may be required to ensure that information from the various studies is gathered and appropriately cataloged and analyzed for use in generic applications.

Using generic information and insights for a plant-specific analysis poses its own set of issues. Foremost is the identification and use of the appropriate information and insights from the generic set relevant to the plant-specific issue being examined.

The major weaknesses associated with simple quantitative evaluations are the scope and level of detail associated with any one particular evaluation. These limitations in scope and level of detail can affect the quality and completeness of any information obtained using such evaluations; thus, decisions made using this type of information may be either conservative or non-conservative–in either case, the decisions are based on information that is not completely realistic.

4.3.2 Tools

This section describes the strengths and weaknesses of the tools that can be used in the non-PRA approach. Specifically, it describes the strengths and weaknesses of the tools for the qualitative approach. Strengths and weaknesses for the other two approaches would be similar to those for the qualitative approach (discussed here) and the plant-specific PRA approach discussed in Section 4.2.2.

Strengths

Safety Monitor, EOOS, and ORAM were specifically designed to facilitate the implementation of defense-in-depth strategies. Thus, several strengths in regard to defense-in-depth are:

- **The capability to accept computer-generated outage schedule information directly**. This feature facilitates the detailed modeling of the multitude of plant configurations created by the outage schedule. Each key safety function is evaluated for each plant configuration defined by the outage schedule.
- **The impact of proposed outage activities on key safety functions can be linked to both the availability of front line systems and to their support system dependencies as well**. All tools are capable of incorporating system dependencies.

- **A color scheme showing the level to which defense-in-depth is achieved for each key safety function is depicted for each plant configuration**. Analysts and outage managers can use these results as a guide to move away from undesirable defense-in-depth situations (e.g., red for any single key safety function or orange in any two) towards a higher level of defense-in-depth (e.g., yellow or green).

Weaknesses

There are no inherent weaknesses to the Safety Monitor, EOOS, or ORAM tools with regard to defense-in-depth principles. Any weaknesses associated with the defense-in-depth output of these tools would be characteristic of the underlying weaknesses of the defense-in-depth method.

REFERENCES

4.1 Nuclear Management and Resources Council, Inc., “Guidelines for Industry Actions to Assess Shutdown Management,” NUMARC 91-06, 1991.

4.2 T. L. Chu, et al., “Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit1 - Analysis of Core Damage Frequency from Internal Events During Mid-Loop Operations,” NUREG/CR-6144, Brookhaven National Laboratory, 1994.

4.3 J.W. Yang, et al., "Risk Comparison of Scheduling Maintenance During Shutdown vs. During Power Operation for PWRs, " NUREG/CR-6616, Brookhaven National Laboratory, Upton, New York, December, 1998.

4.4 T. A. Wheeler, D. W. Whitehead, and E. Lois, “Summary of Information Presented at an NRC-Sponsored Low-Power Shutdown Public Workshop April 27, 1999 Rockville, Maryland,” SAND99-1815, Sandia National Laboratories, July, 1999.

4.5 Electric Power Research Institute, “EOOS, A Tool for Risk Awareness," Version 3.0, November, 1999.

4.6 Electric Power Research Institute, “ ORAM-SETNINEL^{TM} Software Version 3.3," SW-112894-CD M Palo Alto, California.

4.7 SCIENTECH, INC, “Safety Monitor^{TM} Software Version 2.00 Verification and Validation (V&V)," RZ23AF.05c, Kent, Washington, September 1998.

4.8 R. O., Gauntt, et al., “MELCOR Computer Code Manuals,” NUREG/CR-6119, Vol. 1, Rev. 1, Sandia National Laboratories, Albuquerque, New Mexico, July 1997.

4.9 W. T. Pratt, et al., “An Approach for Estimating the Frequencies of Various Containment Failure Modes and Bypass Events,” NUREG/CR-6595, Brookhaven National Laboratory, Upton, New York, 1999.

5. LPSD RESEARCH PLAN

This low power and shutdown (LPSD) research program is to provide (or develop, as necessary) an understanding of the risk associated with LPSD operations sufficient to support risk-informed regulatory decision-making. Looking at the perspectives obtained from the review of low-power and shutdown risk studies and the site visits, the following sections describe the staff's understanding of the risk associated with LPSD operations sufficient to support risk-informed regulatory activities.

Section 5.1 summarizes the information obtained during the review and site visits, and Section 5.2 briefly describes the research issues identified as a result of the review and site visits. To support risk-informed regulatory decision-making, Section 5.3 provides recommendations for methods and guidance development, while schedule and resource requirements are presented in Section 5.4.

5.1 Summary

From the perspectives identified in the previous sections, six high-level observations are made. These observations are discussed below.

Low power and shutdown events are occurring that have the potential to be important given subsequent equipment failures. Numerous events that are potentially risk significant have occurred at United States plants during LPSD conditions. The events have generally involved either a loss of shutdown cooling, loss of coolant, loss of offsite power, or loss of power supplies other than those initiated by loss of offsite power. While the specific causes of the events tend to be plant-specific, the majority of the events include human factors involving either personnel errors and/or deficient procedures.

Risk from low-power and shutdown conditions can be an important component to overall plant risk. Depending on the specific plant, risk (both core damage frequency (CDF) and public) from LPSD conditions can be comparable to full-power. For example, studies presented CDF results in the range of 1E-7 to 8E-5 per year. The most risk-dominant plant operational states are plant-specific, but are usually characterized by high decay heat and reduced inventory.

Using currently available methods and tools, plants have found risk-significant operational states. In their efforts to track and manage shutdown risk (mainly from refueling outages), licensees have developed and used methods and tools to analyze this risk. Using these methods and tools, the plants have identified that they go through risk significant configurations or operational states during refueling outages (e.g., states with reduced water inventory). Identification of these risk-significant states allows the plants to control and minimize the risks from these states.

Current industry practices are valuable for their intended purpose–configuration risk management–but are not sufficient for all potential applications of risk-informed regulatory decision-making. Limitations in current analyses (e.g., simplified thermal-hydraulic calculations used for success criteria development and timing for operator actions) and some of the analysis tools (e.g., the same human reliability analysis (HRA) techniques as used for full-power analyses) may not be appropriate for risk-informed regulatory decision-making that take into account LPSD conditions.

Methods and/or tools are limited in some key areas. Currently, the tools used by industry are limited in a number of areas. They face a lack of sufficient information or guidance on how to deal with selected LPSD issues, such as:

- estimation of source terms in LPSD scenarios,
- calculation of a release risk metric,

- scenarios involving fuel misloading in the spent fuel pool,
- scenarios involving unplanned outages,
- scenarios involving fast reactivity insertions (i.e., boron dilution events),
- scenarios involving crane failure during heavy load lifts,
- inadequate knowledge of how draindown events could occur,
- inadequate knowledge related to cold overpressurization,
- risk associated with the specific activities of moving from one plant operational state to another. One specific aspect of transition risk which also covers the risk from the various stages is going from full power to low power to shutdown, and going back up, and
- appropriate conversion of full-power system models for use in LPSD analyses.

Finally, thermal-hydraulic tools developed for full-power conditions may be inefficient when applied to LPSD conditions.

Available studies provide a strong foundational basis from which to build. Information available from current studies provides valuable insights into those areas which can be risk-significant, as well as areas which may not be risk significant. This information, along with insights pertaining to the strengths and weaknesses of current methods and techniques used to analyze LPSD conditions, provides a mechanism for focusing additional research needed to support risk-informed regulatory decision-making.

5.2 Research Issues

As a result of the information collected and examined during this first information-gathering phase, several research issues have been identified. The research issues, along with a brief discussion of why they are important, are provided below.

Improve the treatment of internal fire and flood and seismic initiators. Previous LPSD analyses have shown that risk from these initiators can be important contributors to specific plants (e.g., an analysis of Surry indicated that fire was a dominant contributor to CDF). As such, it is important to identify the shutdown-specific conditions and activities (i.e., issues) that affect internal fire flood and seismic analyses. Once done, issues that are already adequately examined using current fire, flood, and seismic methodologies should be identified. The effects on CDF and risk of the remaining issues should be prioritized. For those issues deemed a high priority, develop or enhance current techniques to incorporate them into an analysis of shutdown conditions.

Develop techniques for performing a simplified Level 2 risk analysis. To help ensure a more complete understanding of the risk (i.e., beyond CDF) from LPSD conditions and to allow a more direct comparison of the LPSD risk (i.e., public risk) with that from full power, the salient features from the current full-power simplified Level 2 risk analysis process applicable to shutdown conditions should be identified. LPSD conditions should be examined to identify areas requiring additional research sufficient to support these salient features. The research necessary to develop a shutdown-specific simplified Level 2 risk analysis should be performed. The techniques to incorporate a simplified Level 2 risk analysis into a shutdown analysis should be developed or current techniques enhanced, as required.

Improve the treatment of unplanned outages. Generally, LPSD analyses have not examined the risk from unplanned outages. To enhance the completeness of information used in risk-informed decision-making, unplanned outages should be examined. An efficient method for assessing the risk associated with unplanned outages should be developed.

Improve the treatment of transition risk. To enhance the completeness of LPSD analyses, the degree to which transition risk is currently accounted for in shutdown analyses should be identified and the issues associated with transition risk should be investigated and prioritized. For those issues that are deemed a high priority, develop or enhance current techniques to incorporate them into an analysis of shutdown conditions.

Improve the treatment of fast-acting reactivity insertions. At the Sizewell B facility, this issue was found to contribute about 20% of the total fuel damage frequency during shutdown. To help ensure the adequate treatment of this issue, the significance of the following set of issues should be investigated: (1) potential pathways for un-borated water injection, (2) mitigative effects of mixing in the core region and mixing in the piping, and (3) maximum damage that could be expected if a slug of un-borated water moves through the core region. For those issues that are determined to be important, develop or enhance current techniques to incorporate them into an analysis of shutdown conditions, including a quantification methodology.

Improve HRA used for LPSD conditions. Both the NRC and industry analyses have identified the importance of human actions. To help ensure that human actions are adequately analyzed during LPSD conditions, LPSD issues that can affect HRA should be identified and prioritized. For those issues deemed high priority, develop or enhance existing HRA techniques to incorporate into LPSD analyses. Ascertain whether errors-of-commission are important to LPSD risk. If important, develop or enhance current techniques to efficiently model and incorporate errors-of-commission into LPSD analyses.

Improve treatment of crane failures associated with heavy load lifts inside containment. Because accidents resulting from crane failures are not usually included in LPSD analyses, develop or enhance existing techniques to model crane failures during LPSD conditions.

Update crane failure frequencies for heavy load lifts inside containment. To support the improved treatment of crane failures associated with heavy load lifts inside containment, the drop frequencies of nuclear grade crane drops should be updated to account for the past 20 years of nuclear grade crane operating experience.

Establish a LPSD baseline model. To support the use of LPSD risk assessment information in risk-informed regulatory decision-making, a baseline model for LPSD conditions should be developed. The model should account for forced and unplanned outages–at a minimum, accounting for historical forced and unplanned outages.

Improve the current understanding of draindown events and update frequencies. Because past analyses have found that these types of events can be important, past draindown events should be examined to identify factors that influence their occurrence. Initiating event frequencies and uncertainties used in industry and NRC-sponsored LPSD risk analyses should be updated to include post-1990 data. The frequencies should be adjusted to account for the factors that influence their occurrence.

Develop failure data for extended operations. To increase the realism necessary for risk-informed regulatory decision-making, currently available data should be examined to ascertain whether or not it is sufficient to produce failure rate estimates for components that experience extended periods of operation during shutdown conditions. If sufficient information is available, appropriate failure rates should be developed for the components.

Examine current thermal-hydraulic tools to ensure their efficient operation. Thermal-hydraulic calculations play an important roll in determining both success criteria and the time available for operators to respond to events. To increase the usefulness of thermal-hydraulic calculations, developers of the tools used to perform these calculations should be questioned to ascertain whether the tools function efficiently for shutdown conditions. Selected calculations should be performed to verify efficient operation during selected shutdown conditions. If necessary, areas where efficiency is lacking should be addressed by performing code modifications.

Investigate potential for spent fuel pool fuel misloading. Since plants are increasing the storage capacity of their spent fuel pools beyond their original limits and fuel misloading is not usually analyzed as part of a shutdown analysis, a method to assess the risk resulting from these activities should be developed.

Develop guidance on establishing success criteria. Because establishing success criteria is vitally important to correct accident sequence development, LPSD conditions should be examined to identify those that would affect the determination of success criteria. Guidance should then be developed to facilitate the appropriate consideration of these LPSD conditions.

Establish minimum requirements for defining a plant operational state. Defining plant operational states is one task in a LPSD analysis. Currently, different approaches are used, resulting in some analyses having a small number (e.g., 10 to 20) and some having a large number (i.e., much more than 20). To ensure that important parameters are considered when defining plant operational states for LPSD analyses, a workshop should be conducted to develop the minimum set of requirements necessary for defining plant operational states.

Enhance the streamlining of accident sequence analysis. Because LPSD risk has been found to be as important as full-power risk, and because resources should be used effectively to identify the more risk-significant conditions, current information should be examined to identify sets of conditions that generally make a plant state more risk-significant, or conversely, make a plant state less risk-significant. Characteristics of initiating events that can make them important even in a less risk-significant state should also be identified. Once identified, guidelines should be developed to determine which conditions and initiating events should be analyzed. To further enhance the wise use of resources, guidance should be developed on how many plant systems (capable of mitigating an accident sequence) to include in the accident sequence development process.

Develop guidance on how to use full-power models in LPSD analyses. Because of the importance of systems analysis to probabilistic risk assessment (PRA) and because conversion of full-power models for use in LPSD analyses is an efficient use of resources, guidance for converting full-power system models into models for use during LPSD analyses should be developed.

Develop guidance on the correct application of full-power common-cause failure (CCF) models to LPSD conditions. Because correct use or implementation of any PRA model is important, guidance should be developed on what common-cause factors should be reviewed to account for LPSD conditions. Furthermore, specific guidance should be developed on how to adjust full-power CCF models to account for LPSD conditions.

Provide guidance on simplified thermal-hydraulic calculations. Because thermal-hydraulic calculations play an important roll in determining both success criteria and the time available for operators to respond to events, it should be determined whether simplified thermal-hydraulic calculations are sufficient. If simplified calculations are deemed appropriate, then the minimum set of thermal-hydraulic modeling requirements for these simplified calculations should be identified.

Develop guidance on incorporating uncertainty and sensitivity analysis techniques into LPSD analyses. To enhance the usefulness of risk information from LPSD analyses and to provide a more complete understanding of what can be important to risk, guidance on using full-power uncertainty and sensitivity techniques as part of LPSD analyses should be developed.

Develop guidance on cold overpressurization analysis. To enhance the completeness of LPSD analyses, guidelines for incorporating adequate cold overpressurization models should be developed.

5.3 Recommendations

A variety of research issues associated with LPSD risk were discussed above. To provide a sound technical basis for addressing LPSD risk in regulatory decision-making, these research issues can be resolved either through guidance development, method and tool development, or standard development. The priority of the specific issue, however, is dependent on its importance to whether development of a plant-specific LPSD PRA, or some lesser type of LPSD model/approach is needed for the various risk-informed regulatory activities. Therefore, determining which research issues are needed for which approach is the first step in prioritizing the research issues.

Table 5.1 lists each research issue and identifies its importance relative to the type of LPSD information required. A grade is assigned to each issue, whether it is *required* to support the identified approach, whether it is *potentially significant* (may have a significant affect on the successful utilization of the approach), or whether it is *not applicable* (not necessary).

Table 5.1 Importance of research issues relative to LPSD information needed (models).

Tasks (Research Issues)	Importance			
	Development of Plant-Specific PRA	Non PRA		
		Qual./Generic Insights	Qualitative Plant-Specific	Simple Quantitative
Methods				
Fire/Flood/Seismic	Required	Required	Potentially Significant	Required
Simplified Level 2 risk analysis	Required	Required	Potentially Significant	Potentially Significant
Unplanned outages	Required	Required	Potentially Significant	Required
Transition risk	Required	Required	Potentially Significant	Required
Fast-acting reactivity insertions	Required	Required	Potentially Significant	Required
HRA	Required	Required	Potentially Significant	Required
Heavy load lifts	Potentially Significant	Potentially Significant	Not Applicable	Potentially Significant
Crane failure frequency	Potentially Significant	Potentially Significant	Not Applicable	Potentially Significant
LPSD baseline model	Required	Required	Potentially Significant	Required
Understanding of draindown events	Required	Required	Potentially Significant	Required
Extended operation failure data	Required	Required	Not Applicable	Potentially Significant
Thermal-hydraulic tools	Potentially Significant	Potentially Significant	Not Applicable	Potentially Significant
Spent fuel pool fuel misloading	Required	Required	Potentially Significant	Potentially Significant

Table 5.1 Importance of research issues relative to LPSD information needed (models).

Tasks (Research Issues)	Importance			
	Development of Plant-Specific PRA	Non PRA		
		Qual./Generic Insights	Qualitative Plant-Specific	Simple Quantitative
Guidance				
Success criteria	Required	Required	Not Applicable	Potentially Significant
Minimum requirements for defining a POS	Required	Required	Required	Required
Streamlining of accident sequence analysis	Potentially Significant	Potentially Significant	Not Applicable	Potentially Significant
Use of full-power models	Required	Required	Not Applicable	Potentially Significant
Use of full-power CCF models	Required	Required	Not Applicable	Potentially Significant
Simplified thermal-hydraulic calculations	Potentially Significant	Potentially Significant	Not Applicable	Potentially Significant
Uncertainty and sensitivity analysis	Required	Required	Not Applicable	Potentially Significant
Cold overpressurization	Required	Required	Not Applicable	Potentially Significant
Standard	Required	Potentially Significant	Potentially Significant	Potentially Significant

Based on the results in Table 5.1, the following four major tasks are recommended:

(1) Support development of an American Nuclear Society (ANS) LPSD PRA standard. Provide technical expertise in the drafting and finalization of the LPSD standard so that the standard meets NRC needs and can be used to support risk-informed regulatory activities. This task would also involve providing support in the resolution of technical issues important to the development of plant specific PRAs, such as the following:

- requirements for defining a POS.
- success criteria,
- uncertainty and sensitivity analysis,
- cold overpressurization,
- use of full-power models,
- use of full-power CCF models,
- internal floods, and
- internal fire and external seismic

(2) Develop improved guidance for considering LPSD risks. This guidance would be developed for risk-informed licensing decisions (by, for example, supplementing the acceptance guidelines in Regulatory Guide 1.174 to specifically address LPSD risk as previously proposed in SECY-97-287 and Standard Review Plan Chapter 19 to specifically address guidelines for review of LPSD risk analysis), and would be utilized in developing proposed revisions to 10 CFR 50.

(3) Develop improved methods and tools for assessing HRA and Level 2 risk. These areas merit different consideration under LPSD conditions than how they are treated in full-power operation. In addition, a better understanding of these areas is needed because of the large

uncertainties associated with them and because of their potential to directly impact staff risk-informed regulatory activities.

(4) Evaluate areas identified by the ACRS and other stakeholders as potentially important to risk. Development of improved methods or tools for these areas would be to the extent necessary to address the specific technical issue. To the extent possible and appropriate, this work would be performed in cooperative programs with the nuclear industry and NRC's international PRA research partners.[10] Issues would include such items as:

- LPSD baseline model,
- Unplanned outages,
- Transition risk,
- Extended operation failure data,
- Fast acting reactivity insertions,
- Understanding of draindown events,
- Thermal-hydraulic tools,
- Spent fuel pool fuel mis-loading,
- Heavy load lifts, and
- Crane failure frequency.

[10] NRC's International Cooperative PRA Research (COOPRA) Program, initiated in 1997 to identify and perform cooperative research, has a working group on LPSD risk assessment. PRA experts from fifteen countries participate in this working group.

5.4 Schedule and Resources

5.4.1 Schedule

The schedule for the implementation of the recommended issues is set to support the different risk-informed regulatory activities. Therefore, based on the research issues and their relative importance listed in Table 5.1, the following tasks and schedules are planned:

Tasks/Milestones	***Due Date***
1. Support development of ANS LPSD PRA standard	
▸ draft standard	9 - 2000
▸ final standard	6 - 2001
2. Develop preliminary guidance for incorporating LPSD risk into risk-informed regulatory activities:	
▸ Part 50 (proposed rule on special treatment and study of technical requirements)	6 - 2000
▸ Regulatory Guide 1.174 and SRP Chapter 19	12 - 2000
3. Develop improved methods and tools to support risk-informed regulatory activities:	
▸ HRA	6 - 2001 (b)
▸ Level 2	6 - 2001
4. Evaluate areas potentially important to risk: (c)	
▸ LPSD baseline model	FY 2000
▸ Unplanned outages	FY 2001
▸ Transition risk	FY 2001
▸ Extended operation failure data	FY 2001
▸ Fast-acting reactivity insertions	FY 2001
▸ Understanding of draindown events	FY 2001
▸ Thermal-hydraulic tools	FY 2001
▸ Spent fuel pool fuel misloading	FY 2001
▸ Heavy load lifts	FY 2001
▸ Crane failure frequency	FY 2001

Notes:
(a) This work is being performed under the fire and seismic programs, respectively.
(b) This work is being performed under the human reliability analysis program.
(c) Depending on the complexity of the work, this effort may extend beyond FY2001.

5.4.2 Resources

Resources allocated for accomplishing the tasks include the following:

Tasks	***FY 2000***	***FY 2001***
1. Support development of ANS LPSD PRA standard (1)		
▸ Total ($k)	200	100
▸ FTE	0.5	0.5
2. Develop improved guidance (2)		
▸ Total ($k)	100	100
▸ FTE	0.5	0.5
3. Improved methods and tools (3)		
▸ Total ($k)	150	250
▸ FTE	0.5	1.5
4. Evaluate potentially important areas (2) (4)		
▸ Total ($k)	100	500
▸ FTE	0.5	1.0

Notes:
1. ANS has formed a committee to produce an LPSD PRA consensus standard. NRC is actively participating in this effort.
2. For several of the identified research issues, the work will be performed in cooperative programs with the nuclear industry and NRC's international PRA research partners (e.g., NRC's International Cooperative PRA Research (COOPRA) Program, which has a working group on LPSD).
3. The HRA work is costed as part of the HRA research program.
4. The cost assumes that simple methods and tools can be used in the evaluation and, if necessary, developed; however, if more detailed analysis or development is needed, this effort is not included in the cost estimate.

FY2000 resources shown in this table are included in the current RES budget for LPSD and Part 50. Consistent with Commission guidance, FY2001 resources are not included in the agency's budget, as described in the Fiscal Year 2001 Budget Estimates and Performance Plan (Blue Book). Pending a Commission SRM on these recommendations, reprogramming to accommodate additional funding requirements in FY 2001 and resource requirements for FY 2002 will be addressed in the FY 2002 budget formulation process.